PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

SECTION 5
OUTILLAGE POUR LE TRAITEMENT DES RISQUES SSI

Version 2 – 5 février 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)
en collaboration avec le Club EBIOS

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Objet de la modification	Statut
02/1997 (1.1)	Publication du guide d'expression des besoins et d'identification des objectifs de sécurité (EBIOS).	Validé
23/01/2004	Révision globale : - Explications et mise en cohérence avec les normes internationales de sécurité et de gestion des risques - Mise en évidence du référentiel réglementaire par rapport à l'ensemble des contraintes à prendre en compte - Intégration des concepts d'hypothèse et de règles de sécurité (ISO/IEC 15408) - Transfert de la sélection des éléments essentiels dans l'Étude du système-cible - Amélioration de l'élaboration de l'échelle de besoins est améliorée : les valeurs représentant les limites acceptables pour l'organisme par rapport à des impacts personnalisés - Intégration de la détermination des besoins par élément dans l'activité suivante - Intégration de la détermination du mode d'exploitation dans les hypothèses - Adaptation des concepts à l'ISO/IEC 15408 : on étudie l'origine des menaces, c'est-à-dire les méthodes d'attaque et les éléments menaçants, ainsi que leur caractérisation, qui peut inclure un type (naturel, humain, environnemental) une cause (accidentelle, délibérée, en affinant en exposition, ressources disponibles, expertise, motivation), un potentiel d'attaque - Mise en évidence des méthodes d'attaque non retenues - Formalisation des menaces, au sens ISO/IEC 15408 (élément menaçant, attaque et bien sous la forme des entités), avant la confrontation aux besoins de sécurité - Modification de la confrontation des menaces aux besoins, qui permet d'identifier les risques - Mise en évidence des risques non retenus - Intégration de la détermination des objectifs de sécurité minimums dans les activités Formalisation des objectifs de sécurité et Détermination des exigences fonctionnelles - Modification de la détermination des objectifs de sécurité, qui prend en compte les hypothèses, règles de politique de sécurité, contraintes, référentiel réglementaire et risques - Ajout de la détermination des niveaux de sécurité, qui permet de déterminer le niveau des objectifs de sécurité (notamment en fonction des potentiels d'attaque) et de choisir un niveau d'assurance - Ajout de la détermination des exigences de sécurité fonctionnelles, qui permet de déterminer les exigences fonctionnelles couvrant les objectifs de sécurité et de présenter cette couverture - Ajout de la détermination des exigences de sécurité d'assurance, qui permet de déterminer les éventuelles exigences d'assurance Améliorations de forme, ajustements et corrections mineures (grammaire, orthographe, formulations, présentations, cohérence…)	Validé par le Club EBIOS
05/02/2004	Publication de la version 2 du guide EBIOS	Validé

Table des matières

1 Introduction

La méthode EBIOS[1] est composée de cinq sections complémentaires.

- Section 1 – Introduction
  Cette section présente le contexte, l'intérêt et le positionnement de la démarche EBIOS. Elle contient aussi une bibliographie, un glossaire et des acronymes.

- Section 2 – Démarche
  Cette section expose le déroulement des activités de la méthode.

- Section 3 – Techniques
  Cette section propose des moyens de réaliser les activités de la méthode. Il conviendra d'adapter ces techniques aux besoins et pratiques de l'organisme.

- Section 4 – Outillage pour l'appréciation des risques SSI
  Cette section constitue la première partie des bases de connaissances de la méthode EBIOS (types d'entités, méthodes d'attaques, vulnérabilités).

- Section 5 – Outillage pour le traitement des risques SSI
  Cette section constitue la seconde partie des bases de connaissances de la méthode EBIOS (objectifs de sécurité, exigences de sécurité, tableaux de détermination des objectifs et exigences de sécurité fonctionnelles).

Le présent document constitue la cinquième section de la méthode.

Il présente :
- une base d'objectifs de sécurité,
- une base d'exigences de sécurité,
- des tableaux permettant de déterminer les objectifs de sécurité en fonction des menaces (types d'entités, méthodes d'attaque et vulnérabilités) et les exigences de sécurité fonctionnelles pour satisfaire les objectifs de sécurité.

Le tableau suivant présente l'évolution des bases de connaissances fournies dans la section "Outillage" entre la version précédente de la méthode EBIOS et la présente version :

EBIOS v1		**EBIOS v2**	
Objets	**Forme**	**Objets**	**Forme**
Objectifs de sécurité	Classes de fonctionnalités ITSEC	Objectifs de sécurité	Liste d'objectifs de sécurité…
Exigences de sécurité	Rien dans le guide "Outillage"	Exigences de sécurité	Liste d'exigences fonctionnelles de sécurité…
Autres	Tableau croisé des rubriques ITSEC et des menaces, fiche de sélection des menaces, fiches d'expression de la sensibilité des fonctions et informations, fiches de synthèse des besoins de sécurité	Autres	Tableau de détermination des objectifs et exigences de sécurité fonctionnelles

[1] EBIOS est une marque déposée du Secrétariat général de la défense nationale en France.

2 Objectifs de sécurité génériques

Les objectifs de sécurité sont présentés par type d'entités. Ils sont décrits par un code et un libellé. Pour le type d'entités SYS (système), on utilisera les objectifs de sécurité des autres type d'entités.
Bien que l'ensemble de ces objectifs de sécurité ne soit certainement pas exhaustif, il permet de couvrir la majorité des thèmes SSI.
Ces objectifs de sécurité doivent être raffinés afin de les adapter au contexte particulier de l'étude EBIOS.

2.1 MAT : Matériel

Code	Libellé
MAT_01	Il doit exister un stock de matériels de secours en cas de panne d'un équipement
MAT_02	Il doit être possible de restaurer tout ou une partie d'un système, d'une application, d'un ensemble de données et d'une trace en cas de sinistre, de panne ou de négligence
MAT_03	Les modifications modérées de l'environnement (température, humidité, composition de l'air) ne doivent pas induire un comportement anormal des équipements électroniques et des supports
MAT_04	La relecture intègre des supports d'archive doit être garantie pendant toute leur période de conservation
MAT_05	Les équipements et supports doivent pouvoir être ré-exploités à tout moment et dans toute condition, y compris exceptionnelle
MAT_06	La description de tous les équipements informatiques et leur localisation doivent être garanties
MAT_07	Les équipements informatiques et les supports (cartouches de sauvegarde, disques durs, micro-ordinateurs portables) doivent être protégés contre les vols
MAT_08	Toute information sensible destinée à être supprimée d'un support ne doit pas pouvoir être reconstruite
MAT_09	Le dimensionnement des matériels doit être en adéquation avec les services à rendre et tenir compte des périodes éventuelles de surcharge
MAT_10	Les systèmes exploitant les équipements doivent être protégés contre des utilisations par des personnes non autorisées
MAT_11	L'ergonomie et la facilité de maintenance doivent être pris en compte dans le choix des matériels, supports et logiciels
MAT_12	Le matériel doit être conforme aux réglementations hygiène et sécurité en vigueur dans l'entreprise
MAT_13	La supervision et la maintenance des matériels doivent être assurés y compris pendant les périodes de vacances, jours fériés ou hors heures ouvrables
MAT_14	Le respect des exigences de sécurité pour l'installation, l'exploitation et la maintenance des matériels doit être garanti
MAT_15	La fiabilité doit être prise en compte dans le choix des matériels, logiciel et support

2.2 LOG : Logiciel

Code	Libellé
LOG_01	L'intégrité des logiciels et des données doit être garantie
LOG_02	Les mises à jour logicielles ne doivent dégrader ni la sécurité, ni les fonctionnalités des versions antérieures
LOG_03	Toutes les opérations de mises à jour réalisées sur les logicielles doivent être identifiables et justifiables
LOG_04	La configuration des systèmes et applications doit être conforme aux exigences de la politique de sécurité
LOG_05	Toute malveillance ou négligence pesant sur les applications sensibles ainsi que sur les système les hébergeant doit être détectée

Code	Libellé
LOG_06	La mise en production d'un nouvel outil doit être précédée d'une garantie de conformité aux exigences de la politique de sécurité
LOG_07	Il doit exister une gestion des licences, de leur enregistrement et de leur conservation
LOG_08	L'organisme doit maîtriser la liste des configurations installées sur ses équipements et garantir leur conformité dans le temps
LOG_09	Tout logiciel doit être installé conformément aux exigences de sécurité et disposer d'une maintenance assurant sa pérennité
LOG_10	Les traces des opérations doivent être exploitables y compris si elles sont générées par des systèmes différents (possibilité de reconstruire l'enchaînement des événements)
LOG_11	Il doit exister une gestion active des habilitations au sein des systèmes pour le traitement des informations en fonction des besoins d'en connaître et d'en modifier
LOG_12	L'utilisation des moyens de communication ou de travail collaboratif ne satisfaisant pas aux exigences de la politique de sécurité doit être soumise à des conditions et des règles particulières
LOG_13	Tout accès aux systèmes doit être protégé par un dispositif d'authentification et d'identification
LOG_14	Les pannes ou dépassements de performance des systèmes doivent être prévenus
LOG_15	Pour tout système, il doit être possible de détecter en temps réel ou a posteriori un comportement anormal, de retracer les opérations réalisées et d'identifier les auteurs
LOG_16	L'affichage des données sensibles ne doit pas constituer un faille de sécurité pour la confidentialité des données
LOG_17	Les logiciels doivent être conçus de manière à réduire les erreurs d'utilisation

2.3 RES : Réseau

Code	Libellé
RES_01	Les accès aux interfaces de communication doivent être protégés contre une utilisation malveillante ou abusive
RES_02	Les interfaces de communication doivent protéger les transmissions en confidentialité, intégrité et disponibilité
RES_03	L'authentification et la non répudiation des communications doit pouvoir en cas de besoin être établie
RES_04	La compatibilité des éléments interconnectés doit être assurée (langues, fuseaux horaires, normes…)
RES_05	Il doit exister un plan de routage à jour et clair
RES_06	Les accès réseau doivent être prévus et maîtrisés

2.4 PER : Personnel

Code	Libellé
PER_01	Les personnels doivent assurer à l'extérieur des locaux la protection contre le vol ou l'intrusion des équipements et supports
PER_02	Les personnels ayant accès à des informations sensibles doivent être sensibilisés et identifiés
PER_03	Les personnels doivent respecter les bons usages de l'outil informatique, des moyens de communication et de la manipulation des supports ainsi que les dispositions de sécurité associées à la classification des informations
PER_04	Il doit exister un volant de personnel pour assurer la continuité des tâches en cas d'absence
PER_05	Le personnel doit adhérer à la démarche sécurité et les rôles et responsabilités doivent être clairs et connus
PER_06	Les nouveaux personnels ou remplaçants doivent pouvoir assurer leurs tâches en respect de la politique de sécurité
PER_07	Il doit exister une séparation des pouvoirs de décision, d'exécution et de contrôle
PER_08	Le personnel doit être responsabilisé et informé des sanctions encourues

Code	Libellé
PER_09	Le personnel doit être sensibilisé au respect du secret professionnel et de la discrétion
PER_10	Le personnel doit être sensibilisé et formé au respect des normes de l'organisme
PER_11	Le personnel doit montrer des réactions réflexes en cas d'incident (devoir d'information, moyens de remontée de l'information…)
PER_12	Le personnel doit être formé à l'utilisation des matériels et logiciels nécessaires à son activité
PER_13	L'implication de la direction dans la démarche sécurité doit être réelle et visible

2.5 PHY : Site

Code	Libellé
PHY_01	La fourniture des services essentiels au fonctionnement des matériels (i.e. électricité, communication, climatisation…) doit être assurée, de bonne qualité et maîtrisée par l'organisme
PHY_02	Le site ne doit pas permettre l'observation d'informations confidentielles depuis l'extérieur.
PHY_03	Le site et les locaux doivent protéger les matériels contre les agressions, incendies, inondations, perturbations électromagnétiques…
PHY_04	Le choix du site doit permettre de limiter les risques (difficulté d'accès au site, inondation, incendie, pollution, séisme, tempête…) et les intégrer aux pré-requis de construction
PHY_05	Aucune émission électromagnétique compromettante ne doit pouvoir être exploitée depuis l'extérieur des locaux sensibles
PHY_06	Le stockage et la manipulation de matières ou de matériel potentiellement dangereux ne doivent pas induire de risques sur le système d'information
PHY_07	Le site doit être en conformité avec les normes de sécurité de l'organisme
PHY_08	La consommation de tabac, de nourriture, de boisson doit être interdite dans les locaux hébergeant du matériel informatique
PHY_09	Les locaux doivent être protégés contre le déclenchement et la propagation d'incendies
PHY_10	L'installation et l'utilisation du matériel doit se conformer aux standards et normes en vigueur (recommandation du constructeur, règles de la PSSI, normes de sécurité…)
PHY_11	L'installation du matériel doit être planifiée et maîtrisée
PHY_12	Les locaux et leur aménagement doivent être adaptés aux missions de l'organisme

2.6 ORG : Organisation

Code	Libellé
ORG_01	L'organisation doit protéger les équipements et supports contre l'accès physique par des personnes non autorisées
ORG_02	Les procédures d'entrées et sorties doivent lutter contre le vol des matériels
ORG_03	Les moyens de transmission (selon leur nature) et leur exploitation doivent garantir la protection de leur contenu contre les risques de divulgation, de vol, d'altération, de répudiation et de perte
ORG_04	L'organisation doit faire respecter les exigences de la politique de sécurité dans le développement, l'usage et l'exploitation des systèmes (matériels et logiciels)
ORG_05	La politique de restauration doit garantir la reprise intègre des sauvegardes, y compris après l'évolution des systèmes (matériels, logiciels)
ORG_06	La politique anti-virus doit empêcher l'introduction et la diffusion dans les systèmes de tout code malveillant
ORG_07	Une politique d'archivage doit garantir la récupération intègre des données pendant toute la période fixée pour leur conservation
ORG_08	L'organisation doit s'assurer que toutes les données sont sauvegardées selon une fréquence adéquate (y compris des données non centralisées)
ORG_09	L'organisation doit intégrer une politique préventive contre la saturation et les pannes des équipements (informatiques, climatisation, énergie, communication)
ORG_10	L'organisation doit s'assurer de la bonne gestion et de l'utilisation de mots de passe suffisamment robuste

Code	Libellé
ORG_11	La politique de traitement des traces informatiques doit assurer une conformité à la réglementation en vigueur
ORG_12	L'organisation doit lutter contre la réception de messages non sollicités (spam) et contre la désinformation utilisant des moyens de communication interne
ORG_13	L'organisation doit s'assurer de la pérennité des solutions en regard de l'état de l'art et de l'évolution du système d'information
ORG_14	Chaque rôle lié à la sécurité du système d'information doit toujours (même en cas d'absence du titulaire) être placé sous la responsabilité d'au moins une personne ayant les compétences requises ou la possibilité de se référer à une documentation adéquate
ORG_15	L'organisation doit s'assurer de l'identification du caractère confidentiel de toute information et s'assurer de l'application des règles de protection adéquates
ORG_16	L'organisation doit garantir que les moyens de secours sont opérationnels et assurent si cela est possible la continuité de service des activités sensibles de l'organisme en cas de panne, de sinistre ou de malveillance majeure
ORG_17	L'organisation doit s'assurer que les consignes de sécurité seront respectées en cas d'incident ou de malveillance
ORG_18	L'organisation doit garantir que les exigences minimales de sécurité des systèmes d'information sont respectées de tous
ORG_19	L'organisation doit lutter contre la présence de personnes non autorisée sur le site
ORG_20	L'organisation doit contrôler l'intégrité et l'authenticité des fournitures (matériel, logiciel)
ORG_21	L'organisation doit assurer le traitement et le suivi de tout incident de sécurité identifié dans l'organisme
ORG_22	L'organisation doit garantir le contrôle des mesures de sécurité et leur adéquation par rapport aux objectifs de sécurité
ORG_23	L'organisation doit s'assurer de la conformité de tous les locaux avec la politique de sécurité (installation d'une salle technique ou informatique, dispositifs d'accès au site, surveillance des locaux, détection et protection incendie…)
ORG_24	L'organisation doit garantir une réaction rapide et efficace en cas de crise assurant une réduction des impacts potentiels et la continuité des activités essentielles : panne, sinistre, intrusion majeure, autre malveillance
ORG_25	L'organisation doit s'assurer que les interventions de personnes extérieures (prestataires, fournitures…) ne sont pas source de risques pour le système d'information
ORG_26	L'organisation doit garantir le respect de la politique de sécurité lors de la mise en place de tout système sensible (matériel ou logiciel)
ORG_27	L'organisation doit s'assurer que tout matériel ou logiciel est maintenu
ORG_28	L'organisation doit s'assurer de la disponibilité de la documentation technique à jour associée à tout matériel, logiciel, infrastructure
ORG_29	L'organisation doit intégrer un management de la qualité du métier conforme aux normes en vigueur
ORG_30	L'organisation doit lutter contre les accès aux informations et les traitements de données non autorisés
ORG_31	L'organisation de la sécurité du système d'information doit tenir compte du contexte environnant local (économique, social, politique, législatif)
ORG_32	L'organisation doit garantir la prise en compte des besoins de sécurité et des contraintes d'exploitation en amont et tout au long d'un développement
ORG_33	L'organisation doit limiter la possibilité d'abus des droits et privilèges sur les systèmes
ORG_34	L'organisation doit assurer l'accès aux nouvelles technologies aux personnels (formation, partenariat, ..)
ORG_35	L'organisation doit s'assurer de la mise en place d'une politique de sécurité de la protection et de la surveillance des informations
ORG_36	L'organisation doit s'assurer que les procédures mises en place sont suffisamment fluides pour être appliquées

Code	Libellé
ORG_37	L'organisation doit prévoir des sanctions justes et adaptées au contexte en cas de Non-respects de la politique de sécurité qui mettraient en cause la sécurité du système d'information
ORG_38	L'organisation doit s'assurer que ses sous-traitants/prestataires/fournisseurs/industriels/organisations filles/sites respectent la politique de sécurité lors de leurs interventions (travaux, développement, maintenance…)
ORG_39	L'organisation doit s'assurer que les traces et les éléments de preuves sont exploités et protégés en accord avec la politique de sécurité
ORG_40	L'organisation doit s'assurer que l'ensemble des lois et règlements applicables sont pris en compte dans la politique de sécurité
ORG_41	L'organisation doit s'assurer que l'ensemble des règles et procédures applicables est à jour et aisément accessibles par les personnes concernées
ORG_42	L'organisation doit s'assurer que la gestion du système d'information est la plus simple possible
ORG_43	L'exécution des opérations sensibles doit être vérifiée (opérations réalisées par plus d'une personne, validation, exploitation systématique des traces…)
ORG_44	Les risques résiduels acceptés doivent faire l'objet d'études spécifiques et si possible un plan d'action en cas de réalisation doit être élaboré pour chaque risque résiduel identifié
ORG_45	L'organisation doit s'assurer que les conditions de travail sont satisfaisantes

3 Exigences de sécurité fonctionnelles génériques

Les exigences de sécurité fonctionnelles génériques proposées dans cette partie ont été formulées d'après les référentiels suivants :

- l'[ISO 15408],
- l'[ISO 17799],
- diverses sources (EBIOS v1, [PSSI], meilleures pratiques…).

Elles sont présentées par "classe", "famille" et éventuellement "sous-famille" et décrites par un code et un libellé.
Bien que l'ensemble de ces exigences ne soit certainement pas exhaustif, il permet de couvrir la majorité des thèmes SSI.
Ces exigences devront être raffinées afin de les adapter au contexte particulier de l'étude EBIOS.

3.1 Exigences issues de l'ISO 15408

3.1.1 FAU : Audit de sécurité

3.1.1.1 FAU_ARP : Réponse automatique de l'audit de sécurité

Code	Libellé
FAU_ARP.1.1	Des actions d'arrêt de violation et de limitation des impacts doivent être entreprises dès la détection d'une violation potentielle de la sécurité

3.1.1.2 FAU_GEN : Génération des données de l'audit de sécurité

Code	Libellé
FAU_GEN.1.1	Des enregistrements d'audit doivent pouvoir être générés pour des événements spécifiés
FAU_GEN.1.2	Les enregistrements d'audit doivent comprendre au minimum la date, l'heure, le type d'événement, l'identité du sujet, le résultat (succès ou échec) de l'événement ainsi que toute autre information complémentaire nécessaire définie préalablement
FAU_GEN.2.1	Chaque événement auditable doit pouvoir être associé de façon sûre avec l'identité de l'utilisateur qui est à l'origine de l'événement

3.1.1.3 FAU_SAA : Analyse de l'audit de sécurité

Code	Libellé
FAU_SAA.1.1	Des règles doivent permettre d'analyser les événements audités pour détecter des violations potentielles de la sécurité
FAU_SAA.1.2	Les événements auditables indiquant une violation potentielle de la sécurité doivent être identifiés en tant que tel
FAU_SAA.2.1	Des profils types d'utilisation du système représentant les modèles historiques de comportements d'un groupe d'utilisateurs doivent être mise en place et maintenu à jour
FAU_SAA.2.2	Un indice de représentativité à jour doit être associé à chaque utilisateur d'un profil type d'utilisation; il doit indiquer le degré avec lequel l'activité actuelle de l'utilisateur diffère des modèles établis d'utilisation représentés dans le profil
FAU_SAA.2.3	Des règles d'analyse des indices de représentativité afin de détecter de potentielles violations imminentes de la politique de sécurité doivent être mises en place
FAU_SAA.3.1	Une représentation interne d'événements caractéristiques pouvant indiquer une violation de la politique de sécurité doit être maintenue
FAU_SAA.3.2	Un ensemble d'informations à utiliser pour déterminer l'activité du système doit être identifié et comparé aux événements caractéristiques pouvant indiquer une violation de la politique de sécurité
FAU_SAA.3.3	Des mécanismes d'alarme doivent être mis en œuvre pour indiquer une violation imminente de la politique de sécurité quand un événement système se révèle correspondre à un événement caractéristique qui indique une violation potentielle

Code	Libellé
FAU_SAA.4.1	Une représentation interne d'enchaînements d'événements faisant partie de scénarios d'intrusion connus et d'événements caractéristiques doit être maintenue
FAU_SAA.4.2	Les informations utilisées pour déterminer l'activité du système doivent être comparées aux événements caractéristiques et aux enchaînements d'événements
FAU_SAA.4.3	Des mécanismes d'alarme doivent être mis en œuvre pour indiquer une violation imminente de la politique de sécurité quand des événements système se révèlent correspondre à un enchaînement d'événements qui indique une violation potentielle

3.1.1.4 FAU_SAR : Revue de l'audit de sécurité

Code	Libellé
FAU_SAR.1.1	Les utilisateurs autorisés doivent avoir la capacité de consulter les informations d'audits à partir des enregistrements d'audit
FAU_SAR.1.2	Les enregistrements d'audit doivent être présentés d'une façon permettant à l'utilisateur de les interpréter
FAU_SAR.2.1	Le droit d'accès en lecture aux enregistrements d'audit doit être interdit à tous les utilisateurs à l'exception de ceux à qui l'on a accordé un droit de lecture spécifique
FAU_SAR.3.1	Des critères liés logiquement dans les données d'audit doivent être définis de manière à pouvoir effectuer des recherches, des tris et des ordonnancements sur les données d'audit

3.1.1.5 FAU_SEL : Sélection des événements de l'audit de sécurité

Code	Libellé
FAU_SEL.1.1	Des événements auditables doivent pouvoir être exclus des événements audités en fonction de l'identité de l'objet, de l'utilisateur, du sujet ou de l'hôte, du type d'événement ou d'autres attributs sur lesquels se base la sélectivité de l'audit

3.1.1.6 FAU_STG : Stockage d'événements de l'audit de sécurité

Code	Libellé
FAU_STG.1/2.1	Les enregistrements d'audit stockés doivent être protégés contre une suppression non autorisée
FAU_STG.1/2.2	Les modifications effectuées sur les enregistrements d'audit doivent pouvoir être détectées et/ou empêchées
FAU_STG.2.3	Un pourcentage (à définir) des enregistrements d'audit doit être maintenu en cas de dépassement de capacité de stockage des données d'audit, de défaillance ou d'attaque
FAU_STG.3.1	Des actions doivent être prévues si les traces d'audit dépassent une taille limite pré-définie (à définir)
FAU_STG.4.1	Des mesures doivent à mettre en œuvre au cas où la limite de capacité de stockage des données d'audit serait atteinte doivent être définies (par exemple ignorer les événements auditables ou écraser les enregistrements d'audit les plus anciens)

3.1.2 FCO : Communication

3.1.2.1 FCO_NRO : Non-répudiation de l'origine

Code	Libellé
FCO_NRO.1.1	La preuve de l'origine des informations transmises doit pouvoir être générée à la demande de l'émetteur, du destinataire ou de tierces parties (à identifier)
FCO_NRO.1.2	Un lien doit pouvoir être établi entre les attributs de l'émetteur des informations et les champs d'information des informations auxquelles la preuve d'applique
FCO_NRO.1.3	L'émetteur, le destinataire ou des tierces parties (à identifier) doivent avoir la possibilité de vérifier la preuve de l'origine des informations étant donné les limitations relatives à la preuve de l'origine
FCO_NRO.2.1	La preuve de l'origine doit être générée à tout moment pour certains types d'informations transmises (à définir)

3.1.2.2 FCO_NRR : Non-répudiation de la réception

Code	Libellé
FCO_NRR.1.1	La preuve de la réception d'informations transmises doit pouvoir être générée à la demande de l'émetteur, du destinataire ou de tierces parties (à identifier)
FCO_NRR.1.2	Un lien doit pouvoir être établi entre les attributs du destinataire des informations et les champs d'information des informations auxquelles la preuve d'applique
FCO_NRR.1.3	L'émetteur, le destinataire ou des tierces parties (à identifier) doivent avoir la possibilité de vérifier la preuve de la réception des informations étant donné les limitations relatives à la preuve de la réception
FCO_NRR.2.1	La preuve de la réception doit être générée à tout moment pour certains types d'informations transmises (à définir)

3.1.3 FCS : Support cryptographique

3.1.3.1 FCS_CKM : Gestion de clés cryptographiques

Code	Libellé
FCS_CKM.1.1	Les clés cryptographiques doivent être générées conformément à un algorithme de génération de clés cryptographiques spécifiques (à définir) et à des tailles de clés cryptographiques spécifiées (à définir) qui satisfont à des normes identifiées (à définir)
FCS_CKM.2.1	Les clés cryptographiques doivent être distribuées conformément à une méthode de distribution de clés cryptographiques spécifiée (à définir) qui satisfait à des normes identifiées (à définir)
FCS_CKM.3.1	Les types d'accès aux clés cryptographiques doivent être conformes à une méthode d'accès aux lés cryptographiques spécifiée (à définir) qui satisfait à des normes identifiées (à définir)
FCS_CKM.4.1	Les clés cryptographiques doivent être détruites conformément à une méthode de destruction de clés cryptographiques (à définir) qui satisfait à des normes identifiées (à définir)

3.1.3.2 FCS_COP : Opération cryptographique

Code	Libellé
FCS_COP.1.1	Les opérations cryptographiques doivent être exécutées conformément à un algorithme cryptographique (à définir) et avec des tailles de clés cryptographiques spécifiées (à définir) qui satisfont à des normes identifiées (à définir)

3.1.4 FDP : Protection des données de l'utilisateur

3.1.4.1 FDP_ACC : Politique de contrôle d'accès

Code	Libellé
FDP_ACC.1.1	Pour un contrôle d'accès partiel, la politique de sécurité pour les contrôles d'accès doit être appliquées aux sujets, objets et opérations sur les sujets et objets couverts par la politique de sécurité identifiés (à définir)
FDP_ACC.2.1	Pour un contrôle d'accès complet, la politique de sécurité pour les contrôles d'accès doit être appliquées aux sujets, objets identifiés (à définir) et à toutes les opérations sur les sujets et objets couverts par la politique de sécurité
FDP_ACC.2.2	Pour un contrôle d'accès complet, toutes les opérations entre tout sujet et tout objet de la cible sont couverts par la politique de sécurité pour les contrôles d'accès

3.1.4.2 FDP_ACF : Fonctions de contrôle d'accès

Code	Libellé
FDP_ACF.1.1	Pour un contrôle d'accès basé sur les attributs de sécurité, la politique de sécurité pour les contrôles d'accès doit être appliquée aux objets en se basant sur des attributs de sécurité ou des groupes d'attributs de sécurité (à définir)

Code	Libellé
FDP_ACF.1.2	Pour un contrôle d'accès basé sur les attributs de sécurité, les règles qui régissent les accès aux sujets contrôlés et aux objets contrôlés utilisant des opérations contrôlées sur des objets contrôlés doivent toujours être appliquées
FDP_ACF.1.3	Pour un contrôle d'accès basé sur les attributs de sécurité, l'accès de sujets à des objets doit être explicitement autorisé en fonction de règles complémentaires autorisant explicitement ces accès (à définir)
FDP_ACF.1.4	Pour un contrôle d'accès basé sur les attributs de sécurité, l'accès de sujets à des objets doit être explicitement refusé en fonction de règles complémentaires interdisent explicitement ces accès (à définir)

3.1.4.3 FDP_DAU : Authentification de données

Code	Libellé
FDP_DAU.1.2	Des sujets identifiés (à définir) doivent avoir la possibilité de vérifier la preuve de la validité des informations indiquées (à définir)
FDP_DAU.1/2.1	Il doit être possible de générer une preuve pouvant être utilisée comme garantie de la validité d'objets ou de types d'information (à définir)
FDP_DAU.2.2	Pour une authentification avec identité du garant, des sujets identifiés (à définir) doivent avoir la possibilité de vérifier la preuve de la validité des informations indiquées (à définir) et l'identité de l'utilisateur qui a généré la preuve

3.1.4.4 FDP_ETC : Exportation vers une zone hors du contrôle de la TSF

Code	Libellé
FDP_ETC.1.2	Pour une exportation de données sans attributs de sécurité, les données de l'utilisateur doivent être exportées sans les attributs de sécurité associés aux données de l'utilisateur
FDP_ETC.1/2.1	Les politiques de sécurité pour les contrôles d'accès et pour les contrôles de flux d'information doivent être appliquées lors de l'exportation de données de l'utilisateur, contrôlées par la politique de sécurité vers l'extérieur du domaine de sécurité
FDP_ETC.2.2	Pour une exportation de données avec attributs de sécurité, les données de l'utilisateur doivent être exportées avec les attributs de sécurité qui leur sont associés
FDP_ETC.2.3	L'association sans ambiguïté des attributs de sécurité aux données de l'utilisateur doit être garantie quand celles-ci sont exportées
FDP_ETC.2.4	Les règles complémentaires de contrôle d'exportation (à définir) doivent être appliquées lors de l'exportation des données de l'utilisateur vers l'extérieur du domaine de sécurité

3.1.4.5 FDP_IFC : Politique de contrôle de flux d'information

Code	Libellé
FDP_IFC.1.1	Pour un contrôle de flux d'information partiel, la politique de sécurité pour le contrôle de flux d'information doit être appliquée aux sujets, informations et opérations qui déclenchent le transfert vers et en provenance de sujets contrôlés
FDP_IFC.2.1	Pour un contrôle de flux d'information complet, la politique de sécurité pour le contrôle de flux d'information doit être appliquée aux sujets, informations et toutes les opérations qui déclenchent le transfert vers et en provenance de sujets contrôlés
FDP_IFC.2.2	Pour un contrôle de flux d'information complet, toutes les opérations qui déclenchent un transfert d'information vers et en provenance de tout sujet du domaine de sécurité doivent être couvertes par une politique de sécurité pour le contrôle des flux

3.1.4.6 FDP_IFF : Fonctions de contrôle de flux d'information

Code	Libellé

Code	Libellé
FDP_IFF.1.2	Pour des attributs de sécurité simples, un flux d'information entre un sujet contrôlé et des informations contrôlées par l'intermédiaire d'une opération contrôlée doit être autorisé en fonction de règles basées sur les attributs de sécurité (à définir)
FDP_IFF.1/2.1	La politique de sécurité de contrôle de flux doit être appliquée en fonction d'un nombre minimum d'attributs de sécurité identifiés (à définir)
FDP_IFF.1/2.3	Les règles complémentaires de la politique de sécurité pour le contrôle de flux (à définir) doivent être appliquées
FDP_IFF.1/2.4	Une liste des capacités complémentaires de la politique de sécurité (à définir) doit être fournié
FDP_IFF.1/2.5	Un flux d'information doit être explicitement autorisé en fonction de règles basées sur les attributs de sécurité qui autorisent explicitement les flux d'information (à définir)
FDP_IFF.1/2.6	Un flux d'information doit être explicitement interdit en fonction de règles basées sur les attributs de sécurité qui interdisent explicitement les flux d'information (à définir)
FDP_IFF.2.2	Pour des attributs de sécurité hiérarchiques, un flux entre un sujet et des informations contrôlés par l'intermédiaire d'une opération contrôlée doit être autorisé selon des règles basées sur les relations ordonnées entre attributs de sécurité (à définir)
FDP_IFF.2.7.1	Pour des attributs de sécurité hiérarchiques, il doit exister une fonction d'ordonnancement qui, étant donnés deux attributs de sécurité valides, détermine s'ils sont identiques, si l'un et supérieur à l'autre ou s'ils ne sont pas comparables
FDP_IFF.2.7.2	Pour des attributs de sécurité hiérarchiques, il doit exister un "plus petit majorant" tel que, étant donné n'importe quelle paire d'attributs de sécurité valides, il existe un attribut qui est supérieur ou égal aux deux attributs de sécurité valides
FDP_IFF.2.7.3	Pour des attributs de sécurité hiérarchiques, il doit exister un "plus grand minorant" tel que, étant donné n'importe quelle paire d'attributs de sécurité valides, il existe un attribut de sécurité qui n'est pas supérieur aux deux attributs de sécurité
FDP_IFF.3/4.1	L'application de la politique de sécurité pour le contrôle de flux doit pouvoir limiter la capacité des types de flux d'information illicites (à définir) à une capacité maximum (à définir)
FDP_IFF.4.2	Pour une élimination partielle des flux d'information illicites, l'application de la politique de sécurité pour le contrôle de flux doit empêcher certains types de flux illicites identifiés (à définir)
FDP_IFF.5.1	Pour une élimination complète des flux d'information illicites, l'application de la politique de sécurité pour le contrôle de flux doit garantir qu'aucun flux illicite n'existe pour contourner les dispositions de contrôle de flux
FDP_IFF.6.1	La politique de sécurité pour le contrôle de flux doit permettre de surveiller les types de flux illicites (à définir) quand ils dépassent une capacité maximum (à définir)

3.1.4.7 FDP_ITC : Importation depuis une zone hors du contrôle de la TSF

Code	Libellé
FDP_ITC.1.2	Pour une importation sans attribut de sécurité, tout attribut de sécurité associé aux données de l'utilisateur doit être ignoré lors d'une importation depuis l'extérieur
FDP_ITC.1.3/2.5	Les règles complémentaires de la politique de sécurité de contrôle d'importation doivent être appliquées (à définir)
FDP_ITC.1/2.1	La politique de sécurité pour le contrôle d'accès ou pour le contrôle de flux doit être appliquée lors de l'importation de données en provenance de l'extérieur du domaine de sécurité
FDP_ITC.2.2	Pour une importation avec attributs de sécurité, les attributs de sécurité associés aux données de l'utilisateur importées doivent être utilisés
FDP_ITC.2.3	Pour une importation avec attributs de sécurité, le protocole utilisé doit permettre d'associer de façon non ambiguë les attributs de sécurité aux données de l'utilisateur reçues

Code	Libellé
FDP_ITC.2.4	Pour une importation avec attributs de sécurité, l'interprétation des attributs de sécurité des données de l'utilisateur importées doit être celle prévue par l'émetteur des donnes de l'utilisateur

3.1.4.8 FDP_ITT : Transfert interne à la TOE

Code	Libellé
FDP_ITT.1/2.1	La politique de sécurité pour le contrôle d'accès ou pour le contrôle de flux doit empêcher la divulgation, la modification ou la perte d'utilisation des données au cours de leur transmission entre des parties du domaine de sécurité physiquement séparées
FDP_ITT.2.2	Pour une séparation de données transmises en fonction d'attributs, les données contrôlées transmises entre des parties du domaine de sécurité physiquement séparées doivent être séparées en fonction des attributs de sécurité qui exigent une séparation
FDP_ITT.3.1	Les erreurs d'intégrité doivent être détectées au cours de la transmission des données de l'utilisateur entre des parties du domaine de sécurité physiquement séparées
FDP_ITT.3/4.2	En cas de détection d'erreurs d'intégrité, des actions spécifiques (à définir) doivent être entreprises
FDP_ITT.4.1	Pour un contrôle d'intégrité basé sur des attributs, FDP_ITT.3.1 + en fonction des attributs de sécurité qui exigent des canaux de transmission séparés

3.1.4.9 FDP_RIP : Protection des informations résiduelles

Code	Libellé
FDP_RIP.1.1	Pour une protection partielle des informations résiduelles, toute information contenue précédemment dans une ressource doit être rendue indisponible lors de l'allocation ou la désallocation de la ressource à des objets (à définir)
FDP_RIP.2.1	Pour une protection totale des informations résiduelles, toute information contenue précédemment dans une ressource doit être rendue indisponible lors de l'allocation ou de la désallocation de la ressource à tous les objets

3.1.4.10 FDP_ROL : Annulation

Code	Libellé
FDP_ROL.1.1	Pour des annulations élémentaires, l'annulation d'opérations (à définir) sur des objets identifiés (à définir) doit être autorisée
FDP_ROL.1/2.2	Pour des annulations élémentaires, l'annulation des opérations doit être autorisée dans les limites dans lesquelles l'annulation peut être effectuée (à définir)
FDP_ROL.2.1	Pour des annulations avancées, toutes les opérations doivent pouvoir être annulées sur des objets identifiés (à définir)

3.1.4.11 FDP_SDI : Intégrité des données stockées

Code	Libellé
FDP_SDI.1/2.1	Les données de l'utilisateur stockées doivent être contrôlées à la recherche d'erreurs d'intégrité sur tous les objets en fonction des attributs des données de l'utilisateur (à définir)
FDP_SDI.2.1	En cas de détection d'une erreur d'intégrité, des actions spécifiques (à définir) doivent être entreprises

3.1.4.12 FDP_UCT : Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF

Code	Libellé
FDP_UCT.1.1	Les objets doivent être transmis et reçus d'une façon qui les protège d'une divulgation non autorisée

3.1.4.13 FDP_UIT : Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF

Code	Libellé
FDP_UIT.1.1	Les données de l'utilisateur doivent être transmises et reçues d'une façon qui les protège des modifications, suppressions, insertions ou rejeux
FDP_UIT.1.2	Lors de la réception des données de l'utilisateur, il doit être possible de déterminer si une modification, une suppression, une insertion ou un rejeu a eu lieu
FDP_UIT.2.1	Pour une reconstitution grâce à l'émetteur, les données doivent pouvoir être reconstituées à partir d'erreurs compatibles avec une restitution (à définir) avec l'aide du système de confiance à l'origine de l'émission
FDP_UIT.3.1	Pour une reconstitution par le destinataire, les données doivent pouvoir être reconstituées à partir d'erreurs permettant une reconstitution (à définir) sans aucun aide du systèmes de confiance à l'origine de l'émission

3.1.5 FIA : Identification et authentification

3.1.5.1 FIA_AFL : Échecs de l'authentification

Code	Libellé
FIA_AFL.1.1	Le système doit détecter quand un nombre (à définir) de tentatives d'authentification infructueuses ont eu lieu en relation avec des événements liés à l'authentification (à définir)
FIA_AFL.1.2	Des actions spécifiques (à définir) doivent être entreprises quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé

3.1.5.2 FIA_ATD : Définition des attributs de l'utilisateur

Code	Libellé
FIA_ATD.1.1	Une liste d'attributs de sécurité appartenant à des utilisateurs individuels doit être maintenue (à définir)

3.1.5.3 FIA_SOS : Spécification de secrets

Code	Libellé
FIA_SOS.1.1	Un mécanisme doit contrôler que les secrets répondent à une métrique de qualité définie (à définir)
FIA_SOS.2.1	Un mécanisme doit être disponible pour générer des secrets qui répondent à une métrique de qualité définie (à définir)
FIA_SOS.2.2	L'utilisation des secrets générés dans le cadre de FIA_SOS.2.1 doit pouvoir être rendue obligatoire pour des fonctions identifiées (à définir)

3.1.5.4 FIA_UAU : Authentification de l'utilisateur

Code	Libellé
FIA_UAU.1.1	Certaines actions transitant dans le système pour le compte de l'utilisateur (à définir) doivent être autorisées avant que l'utilisateur ne soit authentifié
FIA_UAU.1.2/2.1	Chaque utilisateur doit être authentifié avec succès avant que toute action transitant par le système pour le compte de l'utilisateur ne soit autorisée exceptées les actions définies par le FIA_UAU.1.1
FIA_UAU.3.1	L'utilisation de données d'authentification contrefaites par un utilisateur quelconque doit être détectée et empêchée
FIA_UAU.3.2	L'utilisation de données d'authentification copiées par tout autre utilisateur que l'utilisateur attitré doit être détectée et empêchée
FIA_UAU.4.1	Pour une authentification unique, la réutilisation des données d'authentification liées à des mécanismes d'authentification identifiés (à définir) doit être empêchée
FIA_UAU.5.1	Pour des mécanismes d'authentification multiple, des mécanismes d'authentification multiples (à définir) doivent être fournis pour contribuer à l'authentification de l'utilisateur
FIA_UAU.5.2	Pour des mécanismes d'authentification multiple, l'identité annoncée de tout utilisateur doit être authentifiée selon des règles décrivant comment les mécanismes d'authentification multiple procurent l'authentification (à définir)

Code	Libellé
FIA_UAU.6.1	L'utilisateur doit être réauthentifié dans des conditions spécifiques pour lesquelles une réauthentification est exigée (à définir)
FIA_UAU.7.1	Seules certaines informations spécifiques (à définir) peuvent être fournies à l'utilisateur pendant que l'authentification est en cours

3.1.5.5 FIA_UID : Identification d'un utilisateur

Code	Libellé
FIA_UID.1.1	Certaines actions transitant dans le système pour le compte de l'utilisateur (à définir) doivent être autorisées avant que l'utilisateur ne soit identifié
FIA_UID.1.2/2.1	Chaque utilisateur doit être identifié avec succès avant que toute action transitant par le système pour le compte de l'utilisateur ne soit autorisée exceptées les actions définies par le FIA_UID.1.1

3.1.5.6 FIA_USB : Lien utilisateur-sujet

Code	Libellé
FIA_USB.1.1	Les attributs de sécurité appropriés de l'utilisateur doivent être reliés avec les sujets agissant pour le compte de cet utilisateur

3.1.6 FMT : Administration de la sécurité

3.1.6.1 FMT_MOF : Administration des fonctions de la TSF

Code	Libellé
FMT_MOF.1.1	L'aptitude de déterminer le comportement, désactiver, activer ou modifier le comportement de fonctions identifiées (à définir) doit être restreinte aux rôles autorisés identifiés (à définir)

3.1.6.2 FMT_MSA : Administration des attributs de sécurité

Code	Libellé
FMT_MSA.1.1	L'aptitude de changer la valeur par défaut, d'interroger, de modifier, de supprimer et d'effectuer d'autres opérations identifiées (à définir) certains attributs de sécurité (à définir) doit être restreint aux rôles autorisés identifiés (à définir)
FMT_MSA.2.1	Seules des valeurs sûres doivent être acceptées pour les attributs de sécurité
FMT_MSA.3.1	Les valeurs par défaut restrictives, permissives ou concernant d'autres propriétés (à définir) pour les attributs de sécurité qui sont utilisés pour appliquer la politique de sécurité doivent être fournis
FMT_MSA.3.2	Les rôles autorisés identifiés (à définir) doivent pouvoir spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé

3.1.6.3 FMT_MTD : Administration des données de la TSF

Code	Libellé
FMT_MTD.1.1	L'aptitude de changer une valeur par défaut, d'interroger, de modifier, de supprimer, d'effacer et d'effectuer d'autres opérations identifiées (à définir) certaines données identifiées (à définir) doit être restreinte aux rôles autorisés (à définir)
FMT_MTD.2.1	La spécification des valeurs limites de certaines données (à définir) doit être restreinte aux rôles autorisés identifiés (à définir)
FMT_MTD.2.2	Des actions spécifiques (à définir) doivent être entreprises lorsque les données atteignent les valeurs limites indiquées par le FMT_MTD.2.2 ou les dépassent
FMT_MTD.3.1	Seules des valeurs sûres doivent être acceptées en tant données du système

3.1.6.4 FMT_REV : Révocation

Code	Libellé
FMT_REV.1.1	Seuls les rôles autorisés identifiés (à définir) doivent avoir l'aptitude de révoquer les attributs de sécurité associés aux utilisateurs, sujets, objets et autres ressources complémentaires (à définir) au sein du système

Code	Libellé
FMT_REV.1.2	Des règles spécifiques de révocation (à définir) doivent être mises en œuvre

3.1.6.5 FMT_SAE : Expiration des attributs de sécurité

Code	Libellé
FMT_SAE.1.1	Seuls des rôles autorisés identifiés (à définir) doivent avoir la capacité de spécifier une date d'expiration pour certains attributs de sécurité nécessitant une date d'expiration (à définir)
FMT_SAE.1.2	Certaines actions spécifiques (à définir pour chaque attribut identifié par le FMT_SAE.1.1) doivent pouvoir être entreprises après que la date d'expiration de l'attribut de sécurité est passée

3.1.6.6 FMT_SMR : Rôles pour l'administration de la sécurité

Code	Libellé
FMT_SMR.1/2.1	Les rôles autorisés identifiés (à définir) doivent être tenus à jour
FMT_SMR.1/2.2	Il doit être possible d'associer des utilisateurs à des rôles
FMT_SMR.2.3	Pour des restrictions sur les rôles sécurité, les conditions associées aux différents rôles (à définir) doivent être satisfaites
FMT_SMR.3.1	La prise en charge de certains rôles identifiés (à définir) doivent faire l'objet d'une demande explicite

3.1.7 FPR : Protection de la vie privée

3.1.7.1 FPR_ANO : Anonymat

Code	Libellé
FPR_ANO.1/2.1	Des ensembles d'utilisateurs ou de sujets (à définir) doivent être incapables de déterminer le véritable nom de l'utilisateur associé à des sujets, des opérations ou des objets identifiés (à définir)
FPR_ANO.2.2	Pour un anonymat sans demande d'information, certains services (à définir) doivent être fournis à certains sujets (à définir) sans solliciter une quelconque référence au véritable nom de l'utilisateur

3.1.7.2 FPR_PSE : Possibilité d'agir sous un pseudonyme

Code	Libellé
FPR_PSE.1/2/3.1	Des ensembles d'utilisateurs ou de sujets (à définir) doivent être incapables de déterminer le véritable nom de l'utilisateur associé à des sujets, des opérations ou des objets identifiés (à définir)
FPR_PSE.1/2/3.2	Il doit être possible de fournir un certain nombre d'alias (à définir) du véritable nom de l'utilisateur à des sujets identifiés (à définir)
FPR_PSE.1/2/3.3	Le système doit déterminer un alias pour un utilisateur, accepter l'alias de l'utilisateur et contrôler que l'alias est conforme la métrique relative aux alias (à définir)
FPR_PSE.2.4	Pour une utilisation réversible de pseudonymes, les utilisateurs autorisés et les sujets de confiance (à définir), doivent pouvoir déterminer l'identité de l'utilisateur à partir de l'alias fourni, uniquement sous certaines conditions (à définir)
FPR_PSE.3.4.1	Pour la possibilité d'agir sous un pseudonyme en utilisant un alias, l'alias fourni pour le véritable nom de l'utilisateur doit si possible être identique à un alias fourni précédemment sous certains conditions (à définir)
FPR_PSE.3.4.2	Pour la possibilité d'agir sous un pseudonyme en utilisant un alias, si le FPR_PSE.3.4.1 ne peut être respecté, l'alias fourni doit être sans relation avec les alias précédemment fournis

3.1.7.3 FPR_UNL : Impossibilité d'établir un lien

Code	Libellé

Code	Libellé
FPR_UNL.1.1	Des ensembles d'utilisateurs ou de sujets (à définir) doivent être incapables de déterminer si certaines relations (à définir) ont été déclenchées par le même utilisateur ou sont reliées selon des relations identifiés (à définir)

3.1.7.4 FPR_UNO : Non-observabilité

Code	Libellé
FPR_UNO.1/2.1	Des utilisateurs et des sujets identifiés (à définir) ne doivent pas pouvoir observer l'exécution de certaines opérations (à définir) sur des objets (à définir) par certains utilisateurs et sujet protégés (à définir)
FPR_UNO.2.2	Pour une allocation des informations ayant un impact sur la non-observabilité, les informations relatives à la non-observabilité (à définir) doivent être allouées aux différentes partie du système afin de respecter certaines conditions (à définir)
FPR_UNO.3.1	Certains services (à définir) doivent être fournis à des sujets identifiés (à définir) sans solliciter une quelconque référence à des informations relatives à la vie privée (à définir)
FPR_UNO.4.1	Des utilisateurs autorisés (à définir) doivent avoir la capacité d'observer l'utilisation de ressources ou de services identifiés (à définir)

3.1.8 FPT : Protection de la TSF

3.1.8.1 FPT_AMT : Test de la machine abstraite sous-jacente

Code	Libellé
FPT_AMT.1.1.1	De tests doivent être effectués pendant le démarrage initial pour démontrer le fonctionnement correct des hypothèses de sécurité fournies par les systèmes en charge de la sécurité
FPT_AMT.1.1.2	De tests doivent être effectués pendant le fonctionnement normal pour démontrer le fonctionnement correct des hypothèses de sécurité fournies par les systèmes en charge de la sécurité
FPT_AMT.1.1.3	De tests doivent être effectués à la demande d'un utilisateur autorisé pour démontrer le fonctionnement correct des hypothèses de sécurité fournies par les systèmes en charge de la sécurité
FPT_AMT.1.1.4	De tests doivent être effectués dans certaines conditions complémentaires (à définir) pour démontrer le fonctionnement correct des hypothèses de sécurité fournies par les systèmes en charge de la sécurité

3.1.8.2 FPT_FLS : Mode sûr après défaillance

Code	Libellé
FPT_FLS.1.1	Les systèmes en charge de la sécurité doivent préserver un état sûr quand des types de défaillances (à définir) se produisent

3.1.8.3 FPT_ITA : Disponibilité de données de la TSF exportées

Code	Libellé
FPT_ITA.1.1	La disponibilité de certaines données de sécurité (à définir) fournies à un système de confiance distant dans le cadre d'une métrique de disponibilité spécifique (à définir) étant données des conditions (à définir) pour garantir la disponibilité

3.1.8.4 FPT_ITC : Confidentialité des données de la TSF exportées

Code	Libellé
FPT_ITC.1.1	Toutes les données de sécurité transmise depuis un système en charge de la sécurité vers un système de confiance distant doivent être protégées contre une divulgation non autorisée pendant leur transmission

3.1.8.5 FPT_ITI : Intégrité des données de la TSF exportées

Code	Libellé

Code	Libellé
FPT_ITI.1/2.1	Toute modification de données de sécurité pendant leur transmission entre un systèmes en charge de la sécurité et un système de confiance distant doit être détecté dans la limite d'une métrique de modification spécifique (à définir)
FPT_ITI.1/2.2	L'intégrité de toutes les données sécurité transmises entre un système en charge de la sécurité et un système de confiance distant doit être contrôlée et des actions (à définir) doivent être entreprises si des modifications sont détectées
FPT_ITI.2.3	Pour une correction inter-système d'une modification, des types de modifications (à définir) de toute donnée sécurité transmise entre un système en charge de la sécurité et un système de confiance distant doivent pouvoir être corrigées

3.1.8.6 FPT_ITT : Transfert des données de la TSF à l'intérieur de la TOE

Code	Libellé
FPT_ITT.1/2.1	Les données de sécurité doivent être protégées contre la divulgation et la modification quand elles sont transmises entre des parties séparées du système
FPT_ITT.2.2	Les données de l'utilisateur doivent être séparées des données de sécurité quand de telles données sont transmises entre des parties séparées du système
FPT_ITT.3.1	La modification, la substitution, le ré-ordonnancement, la suppression ou d'autres erreurs d'intégrité (à définir) portant sur les données de sécurité transmises entre des parties séparées du système doivent être détectés
FPT_ITT.3.2	Des actions spécifiques (à définir) doivent être entreprises dès qu'une erreur d'intégrité est détectée sur les données

3.1.8.7 FPT_PHP : Protection physique de la TSF

Code	Libellé
FPT_PHP.1/2.1	Toute intrusion physique susceptible de compromettre la sécurité du système doit être détectée de façon non ambiguë
FPT_PHP.1/2.2	Il doit être possible de déterminer si une intrusion physique dans les dispositifs de sécurité ou dans les éléments de sécurité a eu lieu
FPT_PHP.2.3	Certains dispositifs et éléments de sécurité (à définir) doivent être contrôlés ; toute intrusion physique dans ces dispositifs et éléments doit être notifiée à un utilisateur spécifique ou à un rôle désigné (à définir)
FPT_PHP.3.1	Le système doit résister à des scénarios d'intrusions physiques (à définir) dans des dispositifs ou des éléments de sécurité (à définir) en répondant automatiquement de telle façon que la politique de sécurité ne soit pas violée

3.1.8.8 FPT_RCV : Reprise sûre

Code	Libellé
FPT_RCV.1.1	Après une défaillance ou une interruption de service, les systèmes en charge de la sécurité doivent passer dans un mode de maintenance où l'aptitude de remettre le système dans un état sûr est offerte
FPT_RCV.2/3.1	Quand une reprise automatique à la suite d'une défaillance ou d'une interruption n'est pas possible, les systèmes en charge de la sécurité doivent passer dans un mode de maintenance où l'aptitude de remettre le système dans un état sûr est offerte
FPT_RCV.2/3.2	Pour certaines défaillances ou interruption de service (à définir), le retour du système à un état sûr doit être garanti en utilisant des procédures automatisées
FPT_RCV.3.3	Pour une reprises automatisée sans perte indue, les fonctions pour une reprises à la suite d'une défaillance ou d'une interruption de service doivent garantir que l'état initial sûr est restauré sans dépasser un volume de perte de données (à définir)
FPT_RCV.3.4	Il doit être possible de déterminer les objets qui ont pu ou n'ont pas pu être récupérés
FPT_RCV.4.1	Dans le cas de scénarios de défaillance identifiés (à définir), les fonctions de sécurité doivent soit accomplir leur tâche avec succès, soit reprendre leur fonctionnement dans un état cohérent et sûr

3.1.8.9 FPT_RPL : Détection de rejeu

Code	Libellé
FPT_RPL.1.1	Pour certaines entités identifiées (à définir), le rejeu doit être détecté
FPT_RPL.1.2	Des actions spécifiques (à définir) doivent être exécutées que le rejeu est détecté

3.1.8.10 FPT_RVM : Passage obligatoire par un moniteur de référence

Code	Libellé
FPT_RVM.1.1	Les fonctions qui mettent en œuvre la politique de sécurité doivent être appelées et doivent s'exécuter avec succès avant que chaque fonction du système ne soit autorisée à démarrer

3.1.8.11 FPT_SEP : Séparation de domaines

Code	Libellé
FPT_SEP.1.1	Les systèmes en charge de la sécurité doivent maintenir un domaine de sécurité pour leur propre exécution qui les protège des interférences et des intrusions par des sujets non sûrs
FPT_SEP.1/2/3.2	Une séparation entre les domaines de sécurité de sujets doit être appliquée dans le système
FPT_SEP.2.3	Les systèmes de sécurité en charge des contrôles d'accès ou du contrôle de flux doivent être maintenus dans un domaine de sécurité pour leur propre exécution qui les protège des interférences, des intrusions et des sujets non sûrs
FPT_SEP.2/3.1	La partie non isolée d'un système en charge de la sécurité doit maintenir un domaine de sécurité pour sa propre exécution qui la protège des interférences et des intrusions par des sujets non sûrs
FPT_SEP.3.3	Les parties des systèmes de sécurité en charge des contrôles d'accès ou du contrôle de flux doivent être maintenues dans un domaine de sécurité pour leur propre exécution qui les protège des interférences, des intrusions et des sujets non sûrs

3.1.8.12 FPT_SSP : Protocole de synchronisation d'états

Code	Libellé
FPT_SSP.1/2.1	Un système en charge de la sécurité doit accuser réception d'une transmission sans modification de données de sécurité quand cela est demandé par un autre système en charge de la sécurité
FPT_SSP.2.2	Pour un accusé de réception de confiance mutuel, les systèmes en charge de la sécurité concernés doivent connaître le statut exact des données transmises entre leur différentes parties au moyen d'accusés de réception

3.1.8.13 FPT_STM : Horodatage

Code	Libellé
FPT_STM.1.1	Un système en charge de la sécurité doit être capable de fournir un horodatage fiable pour son propre usage

3.1.8.14 FPT_TDC : Cohérence des données de la TSF inter-TSF

Code	Libellé
FPT_TDC.1.1	Certains types de données de sécurité (à définir) doivent pouvoir être interprétés de façon cohérente quand elles sont partagées entre un système en charge de la sécurité et un système de confiance
FPT_TDC.1.2	Des règles d'interprétation (à définir) doivent être utilisées par les systèmes en charge de la sécurité pour interpréter des données de sécurité d'un autre système de confiance

3.1.8.15 FPT_TRC : Cohérence de la reproduction des données de la TSF à l'intérieur de la TOE

Code	Libellé
FPT_TRC.1.1	Les données de sécurité doivent être cohérentes quand elles sont reproduites entre des parties du système

Code	Libellé
FPT_TRC.1.2	Quand des parties du système contenant des données de sécurité qui ont été reproduites sont déconnectées, la cohérence des données à la reconnexion doit être garantie avant l'exécution de tout fonction de sécurité nécessitant l'utilisation de ces données

3.1.8.16 FPT_TST : Autotest de la TSF

Code	Libellé
FPT_TST.1.1.1	Un système en charge de la sécurité doit exécuter une suite d'autotests pendant le démarrage initial pour démontrer son fonctionnement correct
FPT_TST.1.1.2	Un système en charge de la sécurité doit exécuter une suite d'autotests de façon périodique pendant le fonctionnement normal pour démontrer son fonctionnement correct
FPT_TST.1.1.3	Un système en charge de la sécurité doit exécuter une suite d'autotests à la demande de l'utilisateur autorisé pour démontrer son fonctionnement correct
FPT_TST.1.1.4	Un système en charge de la sécurité doit exécuter une suite d'autotests dans des conditions spécifiques (à définir) pour démontrer son fonctionnement correct
FPT_TST.1.2	Les utilisateurs autorisés doivent avoir la capacité de contrôler l'intégrité des données de sécurité
FPT_TST.1.3	Les utilisateurs autorisés doivent avoir la capacité de contrôler l'intégrité du code exécutable stocké d'un système en charge de la sécurité

3.1.9 FRU : Utilisation des ressources

3.1.9.1 FRU_FLT : Tolérance aux pannes

Code	Libellé
FRU_FLT.1.1	Pour une tolérance aux pannes avec mode dégradé, certaines capacités du système (à définir) doivent être garanties lorsque certaines défaillances (à définir) surviennent
FRU_FLT.2.1	Pour une tolérance aux pannes limitée, toutes les capacités du système doivent être garanties lorsque certaines défaillances (à définir) surviennent

3.1.9.2 FRU_PRS : Priorité de service

Code	Libellé
FRU_PRS.1.2	Pour une priorité de service limitée, chaque accès à des ressources contrôlées (à définir) doit être accordé sur la base de la priorité allouée aux sujets
FRU_PRS.1/2.1	Une priorité doit être affectée à chaque sujet
FRU_PRS.2.2	Pour une priorité de service totale, chaque accès à toutes les ressources partageables doit être accordé sur la base de la priorité allouée aux sujets

3.1.9.3 FRU_RSA : Allocation des ressources

Code	Libellé
FRU_RSA.1/2.1	Des quotas maximums doivent être appliqués pour des ressources contrôlées identifiées (à définir) que des utilisateurs individuels, groupes d'utilisateurs ou sujets (à définir) peuvent utiliser simultanément ou pendant une période de temps spécifiée
FRU_RSA.2.2	Pour des quotas minimums, une quantité minimum de chaque ressource contrôlé identifiée (à définir) doit être disponible pour une utilisation simultanée ou pendant une période de temps spécifiée par un utilisateur, un groupe d'utilisateurs ou des sujets

3.1.10 FTA : Accès à la TOE

3.1.10.1 FTA_LSA : Limitation de la portée des attributs sélectionnables

Code	Libellé

Code	Libellé
FTA_LSA.1.1	La portée des attributs de sécurité de session (à définir) doit être limitée en fonction de certains attributs (à définir)

3.1.10.2 FTA_MCS : Limitation du nombre de sessions parallèles

Code	Libellé
FTA_MCS.1.1	Le nombre maximum de sessions parallèles qui appartiennent au même utilisateur doit être limité
FTA_MCS.1/2.2	Une limite du nombre de sessions par utilisateur (à définir) doit être appliquée par défaut
FTA_MCS.2.1	Pour une limitation du nombre de sessions parallèles par les attributs de l'utilisateur, le nombre maximum de sessions parallèles pour un même utilisateur doit être limité selon des règles (à définir) s'appuyant sur les attributs de l'utilisateur

3.1.10.3 FTA_SSL : Verrouillage de session

Code	Libellé
FTA_SSL.1.1	Une session interactive doit être verrouillée à la suite d'une durée d'inactivité d'un utilisateur (à définir) en rendant le contenu des écrans d'affichage illisibles et en désactivant tout moyen d'accès aux données excepté le déverrouillage de la session
FTA_SSL.1/2.2	Certains événements (à définir) doivent intervenir avant le déverrouillage de la session
FTA_SSL.2.1	L'utilisateur doit pouvoir verrouiller sa propre session interactive en rendant le contenu des écrans d'affichage et en désactivant tout moyen d'accès aux données excepté le déverrouillage de la session
FTA_SSL.3.1	Une session interactive doit être terminée à la suite d'une période d'inactivité d'un utilisateur (à définir)

3.1.10.4 FTA_TAB : Message d'accès à la TOE

Code	Libellé
FTA_TAB.1.1	Avant l'établissement d'une session utilisateur, un message d'avertissement informatif relatif à l'utilisation non autorisée du système doit être affiché

3.1.10.5 FTA_TAH : Historique des accès à la TOE

Code	Libellé
FTA_TAH.1.1	Dès l'établissement réussi d'une session, la date, l'heure, la méthode et le lieu du dernier établissement réussi d'une session doivent être affichés à l'attention de l'utilisateur
FTA_TAH.1.2	Dès l'établissement réussi d'une session; la date, l'heure, la méthode et le lieu de la dernière tentative d'établissement infructueuse d'une session et le nombre de tentative infructueuse depuis le dernier établissement réussi doit être affiché
FTA_TAH.1.3	Les informations concernant l'historique des accès ne doivent pas être effacées de l'interface utilisateur sans laisser à l'utilisateur la possibilité de revoir ces informations

3.1.10.6 FTA_TSE : Établissement d'une session de la TOE

Code	Libellé
FTA_TSE.1.1	L'établissement d'une session doit pouvoir être refusé en fonction de certains attributs (à définir)

3.1.11 FTP : Chemins et canaux de confiance

3.1.11.1 FTP_ITC : Canal de confiance inter-TSF

Code	Libellé

Code	Libellé
FTP_ITC.1.1	Un canal de communication logiquement distinct des autres canaux et garantissant l'indentification de ses extrémités et la protection des données en transit contre la modification ou la divulgation doit être fourni avec chaque système de confiance
FTP_ITC.1.2	La communication via un canal de confiance doit pouvoir être initiée par le système ou par le système de confiance concerné
FTP_ITC.1.3	Le système doit initier la communication via le canal de confiance pour des fonctions pour lesquelles un canal de confiance est exigé (à définir)

3.1.11.2 FTP_TRP : Chemin de confiance

Code	Libellé
FTP_TRP.1.1	Un chemin de communication logiquement distinct des autres chemins et garantissant l'indentification de ses extrémités et la protection des données en transit contre la modification ou la divulgation doit être fourni le système et un utilisateur
FTP_TRP.1.2	La communication via un chemin de confiance doit pouvoir être initiée par le système, par des utilisateurs locaux ou par des utilisateurs distants
FTP_TRP.1.3	L'utilisation du chemin de confiance doit être exigée pour l'authentification initiale d'un utilisateur et pour d'autres services (à définir)

3.2 Exigences issues de l'ISO 17799

3.2.1 BPS : Politique de sécurité (Chapitre 3)

3.2.1.1 BPS_PSI : Politique de sécurité de l'information (§3.1)

Code	Libellé
BPS_PSI.1.1	Une documentation de politique de sécurité doit être élaborée et approuvée par la direction
BPS_PSI.1.2	La politique de sécurité doit être diffusée à l'ensemble des collaborateurs
BPS_PSI.1.3	La politique de sécurité doit inclure la définition des responsabilités générales et spécifiques
BPS_PSI.1.4	La politique de sécurité doit définir des règles de sécurité claires et applicables couvrant l'ensemble des aspects de la sécurité
BPS_PSI.1.5	La politique de sécurité doit contenir des règles sur la classification de l'information
BPS_PSI.2.1.1	La politique de sécurité doit être examinée régulièrement et en cas de changements qui l'influencent, pour faire en sorte qu'elle continue d'être appropriée
BPS_PSI.2.1.2	La mise à jour de la politique de sécurité doit être de la responsabilité d'un groupe ou comité de revue dont les membres sont identifiés
BPS_PSI.2.1.3	Le groupe ou comité de revue de la politique de sécurité doit s'appuyé sur les travaux du groupe de gestion de la sécurité (voir BOS_ISI.1.2)
BPS_PSI.2.2	La conformité des systèmes d'information avec la politique de sécurité doit être examinée avant toute ouverture de nouveaux services du SI
BPS_PSI.2.3	Il doit exister une procédure de remise en cause de la politique ou des règles de sécurité en fonction des informations recueillies sur les incidents de sécurité signalés (type, fréquence, coûts induits…)
BPS_PSI.2.4	L'adéquation de la politique de sécurité avec les enjeux métiers doit être régulièrement vérifiée (par exemple dans le cadre d'une politique d'audit globale)

3.2.2 BOS : Organisation de la sécurité (Chapitre 4)

3.2.2.1 BOS_ISI : Infrastructure de la sécurité de l'information (§4.1)

Code	Libellé
BOS_ISI.1.1	Un groupe de gestion de la sécurité doit être établi de façon à donner une orientation claire et à fournir un soutien visible de la direction aux initiatives de sécurité
BOS_ISI.1.2	Le groupe de gestion de la sécurité doit s'appuyer sur des états périodiques de la sécurité des systèmes d'information (incidents relevés, avancement des plans d'action, nouveaux services…)
BOS_ISI.2.1	Si possible, la coordination de la mise en œuvre des mesures de maîtrise de sécurité de l'information doit être prise en charge par un groupe de gestion dont les membres représentent des fonctions diverses dans les sections concernées de l'organisme
BOS_ISI.3.1	Les responsabilités concernant la protection du capital individuel et des informations ainsi que l'exécution de processus de sécurité spécifiques doivent être clairement définies
BOS_ISI.3.2	La politique de sécurité doit donner des lignes directrices générales pour l'attribution des responsabilités sécurité.
BOS_ISI.3.3	Les lignes directrices de la politique de sécurité pour l'attribution des responsabilités sécurité peuvent être complétées par des documents complémentaires plus détaillés pour des sites, des systèmes ou des services spécifiques
BOS_ISI.4.1	Un processus d'autorisation par la direction pour les nouvelles infrastructures de traitement de l'information doit être établi

Code	Libellé
BOS_ISI.5.1	L'organisme doit disposer d'une veille technologique adaptée à ses environnements et à ses enjeux (suivi des vulnérabilités et des correctifs par exemple)
BOS_ISI.5.2	Il doit être possible de demander conseil à des spécialistes internes ou externes (y compris des organismes nationaux spécialisés en sécurité des systèmes d'information tels que la DCSSI ou la CNIL) au sujet de la sécurité de l'information
BOS_ISI.5.3	Les conseils obtenus auprès de spécialistes doivent être communiqués dans toute l'organisation
BOS_ISI.6.1	Il faut maintenir des contacts appropriés avec les autorités légales, les organismes de réglementation, les prestataires de services informatiques et les exploitants des télécommunications
BOS_ISI.6.2	En cas d'incident de sécurité, les contacts précisés dans le BOS_ISI.6.1 doivent pouvoir être utilisés afin d'assurer une réaction rapide et appropriée (obtention de conseils, action des partenaires…)
BOS_ISI.6.3	Les échanges avec les contacts précisés dans le BOS_ISI.6.1 ne doivent pas mettre en péril la protection des informations de sécurité
BOS_ISI.7.1	La mise en application de la politique de sécurité de l'information doit faire l'objet d'une revue indépendante (par exemple par un organisme interne ou externe qui n'a pas d'autre responsabilité opérationnelle dans le domaine de la sécurité)

3.2.2.2 BOS_SAT : Sécurité des accès par des tiers (§4.2)

Code	Libellé
BOS_SAT.1.1	Un inventaire de la nature des accès au système d'information par des tiers (accès logiques et accès physiques) doit être réalisé et une analyse de risque doit être menée pour chacun des accès répertoriés
BOS_SAT.1.2	Des mesures appropriées de maîtrise de la sécurité des accès au système d'information par des tiers doivent être mises en œuvre
BOS_SAT.1.3	A chaque fois qu'un tiers doit intervenir sur le système d'information, un responsable de l'organisme doit disposer de moyens de contrôler les opérations réalisées
BOS_SAT.1.4	L'accès au système d'information par des tiers doit être motivé par un besoin fonctionnel
BOS_SAT.1.5	L'accès au système d'information par des tiers intervenant sur site ne doit pas être mis en place avant que des mécanismes de contrôle appropriés ne soient mis en œuvre et qu'un contrat définissant les modalités d'accès ne soit signé
BOS_SAT.2.1	Les dispositions impliquant l'accès par des tiers aux infrastructures de traitement de l'information de l'organisme doivent être basées sur un contrat en bonne et due forme contenant toutes les exigences de sécurité nécessaires

3.2.2.3 BOS_SOT : Sous-traitance(§4.3)

Code	Libellé
BOS_SOT.1.1	Les exigences de sécurité d'un organisme confiant à des tiers la gestion et la maîtrise de tout ou partie de ses systèmes informatiques, ses réseaux et/ou ses environnements de bureau doivent être abordées dans un contrat convenu entre les parties
BOS_SOT.1.2	Les contrats de services externalisés doivent définir les responsabilités des contractants et les recours possibles en cas de défaillances à cet accord

3.2.3 BCM : Classification et contrôle des actifs (Chapitre 5)

3.2.3.1 BCM_RLC : Responsabilités liées aux actifs (§5.1)

Code	Libellé
BCM_RLC.1.1	Un inventaire global des biens et ressources (y compris les licences associées) permettant au moins d'identifier les éléments sensibles et vitaux doit être dressé

3.2.3.2 BCM_CLI : Classification de l'information (§5.2)

Code	Libellé
BCM_CLI.1.1	Les classifications et les mesures de protection associées ayant trait à l'information devront tenir compte des besoins de l'entreprise de partager ou de restreindre l'information et des impacts professionnels relatifs à ces besoins
BCM_CLI.1.2	Si possible, la responsabilité de l'attribution d'une classification à une information et de la revue périodique de cette classification doit incombée à l'émetteur de l'information ou à son propriétaire attitré
BCM_CLI.2.1	Un ensemble de procédures doit être défini pour l'étiquetage et le traitement de l'information conformément au système de classification adopté par l'organisme

3.2.4 BSP : Sécurité du personnel (Chapitre 6)

3.2.4.1 BSP_SPR : Sécurité dans la définition des postes et des ressources (§6.1)

Code	Libellé
BSP_SPR.1.1	Les rôles et les responsabilités en matière de sécurité, tels qu'ils sont décrits dans la politique de sécurité de l'organisme doivent être documentés dans les définitions des postes dans la mesure du possible
BSP_SPR.2.1	Les contrôles de vérification concernant le personnel permanent doivent être effectués au moment de la demande d'emploi
BSP_SPR.3.1	Les employés doivent signer un accord de confidentialité comme faisant partie de leurs conditions initiales d'emploi
BSP_SPR.4.1	Les conditions d'emploi devront stipuler la responsabilité de l'employé en matière de sécurité

3.2.4.2 BSP_FOU : Formation des utilisateurs (§6.2)

Code	Libellé
BSP_FOU.1.1	Tous les employés de l'organisme et, le cas échéant, les utilisateurs extérieurs à l'organisme, doivent recevoir une formation appropriée et des mises à jour régulières sur la politique de sécurité et les procédures de l'organisme
BSP_FOU.2.1	Tous les employés de l'organisme et, le cas échéant, les utilisateurs extérieurs à l'organisme, doivent recevoir une formation appropriée sur l'utilisation des outils (notamment à la mise en production de nouveaux outils)

3.2.4.3 BSP_RIS : Réaction aux incidents de sécurité et aux défauts de fonctionnement (§6.3)

Code	Libellé
BSP_RIS.1.1	Les incidents de sécurité doivent être signalés par l'intermédiaire des filières de gestion appropriées dès que possible après leur découverte
BSP_RIS.2.1	Les utilisateurs de services d'information doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou les services ou toute menace à laquelle ces derniers seraient exposés
BSP_RIS.3.1	Des procédures pour le signalement du mauvais fonctionnement de logiciels devront être établies et suivies
BSP_RIS.4.1	Des mécanismes doivent être mis en place afin de permettre de quantifier et de contrôler les types, les volumes et le coût des incidents et des mauvais fonctionnements
BSP_RIS.5.1	La violation de la politique sécurité et des procédures de sécurité de l'organisme par des employés devra être traitée au moyen d'un processus disciplinaire
BSP_RIS.5.2	Les mesures disciplinaires pour violation de la politique sécurité et des procédures de sécurité doivent être communiquées à tous les employés

3.2.5 BPE : Sécurité physique et sécurité de l'environnement (Chapitre 7)

3.2.5.1 BPE_ZOS : Zones de sécurité (§7.1)

Code	Libellé

Code	Libellé
BPE_ZOS.1.1	Les organismes doivent utiliser des périmètres de sécurité pour protéger les zones qui contiennent des infrastructures de traitement de l'information
BPE_ZOS.2.1	Les zones de sécurité doivent être protégées par des mesures de maîtrise appropriées à l'entrée pour faire en sorte que seul le personnel autorisé puisse y avoir accès
BPE_ZOS.3.1	Des zones de sécurité doivent être créées afin de protéger les bureaux, les salles et les infrastructures ayant des exigences de sécurité spéciales
BPE_ZOS.4.1	Des mesures de maîtrise et des directives supplémentaires pour le travail dans les zones de sécurité doivent être utilisées pour augmenter la sécurité fournie par les mesures de maîtrise physiques protégeant les zones de sécurité
BPE_ZOS.5.1	Les zones de livraison et de chargement doivent être maîtrisées et si possible isolées des infrastructures de traitement de l'information afin d'éviter tout accès non autorisé

3.2.5.2 BPE_SEM : Sécurité du matériel (§7.2)

Code	Libellé
BPE_SEM.1.1	Le matériel informatique doit être situé et protégé de façon à réduire les risques présentés par les menaces et les dangers liés à l'environnement et les occasions d'accès non autorisés
BPE_SEM.2.1	Le matériel doit être protégé contre les pannes de courant ou les autres anomalies électriques
BPE_SEM.3.1	Le câblage électrique et de télécommunication transmettant des données ou supportant des services d'information doit être protégé contre les interceptions
BPE_SEM.3.2	Le câblage électrique et de télécommunication transmettant des données ou supportant des services d'information doit être protégé contre les dommages
BPE_SEM.4.1	Le matériel doit être entretenu conformément aux instructions du fabricant et/ou aux procédures documentées afin d'assurer sa disponibilité et son intégrité continues
BPE_SEM.5.1	Des procédures et des mesures de maîtrise de sécurité doivent être utilisées afin de sécuriser le matériel utilisé à l'extérieur des locaux d'un organisme
BPE_SEM.6.1	Les informations contenues sur un matériel doivent être effacées avant sa mise au rebut ou sa réutilisation

3.2.5.3 BPE_MMG : Mesures de contrôle générales (§7.3)

Code	Libellé
BPE_MMG.1.1	Les organismes doivent adopter et appliquer une politique de bureaux et d'écrans dégagés afin de réduire les risques d'accès non autorisé, de perte d'informations et de dommages subis par les informations
BPE_MMG.2.1	Aucun matériel, aucune information ni aucun logiciel ne doivent être enlevés sans autorisation

3.2.6 BGC : Gestion des communications et des opérations (Chapitre 8)

3.2.6.1 BGC_PRE : Procédures et responsabilités opérationnelles (§8.1)

Code	Libellé
BGC_PRE.1.1	Les procédures opérationnelles doivent être documentées et maintenues
BGC_PRE.2.1	Les modifications apportées aux infrastructures de traitement de l'information et aux systèmes informatiques doivent être contrôlées par les responsables des infrastructures concernées
BGC_PRE.2.2	Les modifications apportées aux infrastructures de traitement de l'information et aux systèmes informatiques doivent être documentées
BGC_PRE.3.1	Des responsabilités et des procédures de gestion des incidents doivent être établies de façon à assurer une réaction rapide, efficace et ordonnées aux incidents de sécurité

Code	Libellé
BGC_PRE.4.1	Les responsabilités et les zones de responsabilité doivent être divisées de façon à réduire les possibilités de modifications non autorisées ou d'utilisation abusive de l'information ou des services
BGC_PRE.5.1	Les infrastructures de développement et d'essai devront être séparées des infrastructures opérationnelles
BGC_PRE.6.1	Avant d'utiliser des services externes de gestion des infrastructures, les risques doivent être identifiés à l'avance et des mesures de maîtrise appropriées doivent être convenues avec le fournisseur et incluses dans le contrat

3.2.6.2 BGC_PRS : Planification et recette des systèmes (§8.2)

Code	Libellé
BGC_PRS.1.1	Les demandes en capacité doivent être surveillées et des prévisions sur les besoins de capacité futurs doivent être faites afin d'assurer la disponibilité d'une puissance de traitement et d'un stockage adéquats
BGC_PRS.2.1	Des critères de recette pour les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions doivent être établis et des essais adéquats du système doivent être effectués avant sa recette

3.2.6.3 BGC_PLM : Protection contre les logiciels malveillants (§8.3)

Code	Libellé
BGC_PLM.1.1	Des mesures de maîtrise de détection et de prévention doivent être mises en œuvre afin de fournir une protection contre les logiciels malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs doivent être mises en œuvre

3.2.6.4 BGC_INT : Intendance (§8.4)

Code	Libellé
BGC_INT.1.1	Des copies de sauvegarde des informations professionnelles et des logiciels essentiels doivent être faites à intervalles réguliers
BGC_INT.2.1	Le personnel opérationnel doit tenir un journal de ses activités
BGC_INT.3.1	Les défauts doivent être signalés et des mesures correctives doivent être prises

3.2.6.5 BGC_GER : Gestion des réseaux (§8.5)

Code	Libellé
BGC_GER.1.1	Un ensemble de mesures de maîtrise doit être mis en œuvre afin d'obtenir et de maintenir la sécurité dans les réseaux

3.2.6.6 BGC_MSS : Manipulation et sécurité des supports (§8.6)

Code	Libellé
BGC_MSS.1.1	La gestion des supports informatiques amovibles, tels que les bandes, les disques, les cassettes et les rapports imprimés doit être maîtrisée
BGC_MSS.2.1	Les supports informatiques doivent être mis au rebut d'une manière sûre lorsqu'ils sont devenus inutiles
BGC_MSS.3.1	Des procédures pour la manipulation et le stockage des informations doivent être établies afin de protéger ces informations contre toute divulgation non autorisée ou toute utilisation abusive.
BGC_MSS.4.1	La documentation des systèmes doit être protégée contre tout accès non autorisé

3.2.6.7 BGC_EIL : Échanges d'informations et de logiciels (§8.7)

Code	Libellé
BGC_EIL.1.1	Des accords, dont certains peuvent être officiels, doivent être établis pour les échanges d'informations et de logiciels entre organismes
BGC_EIL.2.1	Les supports en transit doivent être protégés contre tout accès non autorisé, toute utilisation abusive ou toute altération

Code	Libellé
BGC_EIL.3.1	Le commerce électronique doit être protégé contre les activités frauduleuses, les différends contractuels et la divulgation ou la modification de l'information
BGC_EIL.4.1	Une politique doit être élaborée pour l'utilisation du courrier électronique et des mesures de maîtrise doivent être mises en place afin de réduire les risques de sécurité créés par le courrier électronique
BGC_EIL.5.1	Des politiques et des indications doivent être élaborées et mises en œuvre afin de maîtriser les risques professionnels et les risques de sécurité associés aux systèmes bureautiques
BGC_EIL.6.1	Il doit y avoir un processus d'autorisation officielle avant que des informations soient rendues disponibles au public et l'intégrité de ces informations doit être protégée contre toute modification non autorisée
BGC_EIL.7.1	Des procédures et des mesures de maîtrise doivent être en place pour protéger l'échange d'informations par des moyens de communication vocale, par télécopie et vidéo

3.2.7 BMA : Contrôle des accès (Chapitre 9)

3.2.7.1 BMA_EMA : Exigences de l'entreprise concernant le contrôle des accès (§9.1)

Code	Libellé
BMA_EMA.1.1	Les exigences professionnelles de maîtrise d'accès doivent être définies et documentées et l'accès doit être limité à ce qui est défini dans la politique de maîtrise des accès

3.2.7.2 BMA_GAU : Gestion des accès utilisateurs (§9.2)

Code	Libellé
BMA_GAU.1.1	Il doit y avoir une procédure officielle d'enregistrement et de désenregistrement des utilisateurs pour l'octroi de l'accès à tous les systèmes et les services informatiques multi-utilisateurs
BMA_GAU.2.1	L'attribution et l'utilisation de privilèges doivent être restreintes et maîtrisées
BMA_GAU.3.1	L'attribution des mots de passe doit être maîtrisée par un processus de gestion officiel
BMA_GAU.4.1	Un processus officiel de revue des droits d'accès des utilisateurs doit être exécuté à des intervalles réguliers

3.2.7.3 BMA_REU : Responsabilités des utilisateurs (§9.3)

Code	Libellé
BMA_REU.1.1	Les utilisateurs doivent suivre de bonnes pratiques sécurité lors de la sélection et de l'utilisation des mots de passe
BMA_REU.2.1	Les utilisateurs doivent veiller à ce que le matériel sans surveillance ait une protection sécuritaire appropriée

3.2.7.4 BMA_MAR : Contrôle de l'accès aux réseaux (§9.4)

Code	Libellé
BMA_MAR.1.1	Les utilisateurs ne doivent pouvoir accéder directement qu'aux services spécifiques qu'ils ont été autorisés à utiliser
BMA_MAR.2.1	L'itinéraire entre le terminal utilisateur et le service informatique doit être maîtrisé
BMA_MAR.3.1	L'accès par des utilisateurs éloignés doit donner lieu à une authentification
BMA_MAR.4.1	Les connexions faites à des systèmes informatiques à distance doivent être authentifiées
BMA_MAR.5.1	L'accès aux ports de diagnostic doit être maîtrisé de façon sûre
BMA_MAR.6.1	Des mesures de maîtrise doivent être introduites dans les réseaux afin d'isoler des groupes de services d'information, d'utilisateurs et de systèmes d'information
BMA_MAR.7.1	La capacité de connexion des utilisateurs doit être restreinte dans les réseaux partagés, conformément à la politique de maîtrise des accès du BMA_EMA.1.1

Code	Libellé
BMA_MAR.8.1	Les réseaux partagés doivent avoir des mesures de maîtrise de routage pour faire en sorte que les connexions d'ordinateurs et le flux des informations n'enfreignent pas le BMA_EMA.1.1
BMA_MAR.9.1	Une description claire des caractéristiques de sécurité de tous les services utilisés par l'organisme doit être fournie

3.2.7.5 BMA_MAS : Contrôle de l'accès aux systèmes d'exploitation (§9.5)

Code	Libellé
BMA_MAS.1.1	Une identification automatique du terminal doit être utilisée pour authentifier les connexions à des sites spécifiques et au matériel portable
BMA_MAS.2.1	L'accès aux services d'information doit se faire par l'intermédiaire d'un processus de connexion sûr
BMA_MAS.3.1	Tous les utilisateurs doivent avoir un identificateur unique (code d'identification utilisateur) pour leur utilisation personnelle exclusive, de sorte que les activités puissent être associées rétrospectivement à l'individu responsable
BMA_MAS.4.1	Les systèmes de gestion des mots de passe doivent fournir une fonction interactive efficace qui assure la qualité des mots de passe (pas de mots de passe trop courts ou trop simples, pas de réutilisation de mots de passe précédents…)
BMA_MAS.5.1	L'utilisation de programmes utilitaires doit être restreinte et étroitement maîtrisée
BMA_MAS.6.1	Un avertisseur individuel doit être fourni aux utilisateurs qui pourraient faire l'objet de coercition
BMA_MAS.7.1	Les terminaux non utilisés situés dans des zones à hauts risques ou desservant des systèmes à hauts risques doivent s'éteindre automatiquement après une période d'inactivité déterminée afin d'empêcher que des personnes non autorisées y accèdent
BMA_MAS.8.1	La limitation du temps de connexion doit être utilisée afin de fournir un niveau de sécurité supplémentaire pour les applications à hauts risques

3.2.7.6 BMA_MAA : Contrôle de l'accès aux applications (§9.6)

Code	Libellé
BMA_MAA.1.1	Les accès à l'information et aux fonctions des systèmes d'applications doivent être limités conformément à la politique de maîtrise d'accès du BMA_EMA.1.1
BMA_MAA.2.1	Les systèmes critiques doivent avoir un environnement informatique dédié (isolé)

3.2.7.7 BMA_SAS : Surveillance des accès aux systèmes et de leur utilisation (§9.7)

Code	Libellé
BMA_SAS.1.1	Des journaux d'audit où sont enregistrés les exceptions et les autres événements relatifs à la sécurité doivent être produits et tenus pendant une période convenue de façon à faciliter les enquêtes futures et le contrôle des mesures de maîtrise des accès
BMA_SAS.2.1	Des procédures pour la surveillance de l'utilisation des infrastructures de traitement de l'information doivent être établies et le résultat de ces activités de surveillance doit être examiné régulièrement
BMA_SAS.3.1	Les horloges des ordinateurs doivent être synchronisées afin d'obtenir un enregistrement exact

3.2.7.8 BMA_IMT : Informatique mobile et télétravail (§9.8)

Code	Libellé
BMA_IMT.1.1	Une politique officielle doit être établie et des mesures de maîtrise appropriées doivent être adoptées afin de fournir une protection contre les risques présentés par le travail avec des unités informatiques mobiles.
BMA_IMT.2.1	Des politiques et des procédures doivent être établies pour l'autorisation et la maîtrise des activités de télétravail

3.2.8 BDM : Développement et maintenance des systèmes (Chapitre 10)

3.2.8.1 BDM_ESS : Exigences de sécurité des systèmes (§10.1)

Code	Libellé
BDM_ESS.1.1	Les exigences de l'entreprise pour de nouveaux systèmes ou les améliorations apportées à des systèmes existants doivent spécifier les exigences relatives aux mesures de maîtrise

3.2.8.2 BDM_SSA : Sécurité des systèmes d'applications (§10.2)

Code	Libellé
BDM_SSA.1.1	Les données d'entrée des systèmes d'applications doivent être validées pour faire en sorte qu'elles soient correctes et appropriées
BDM_SSA.2.1	Des vérifications de validation doivent être incorporées dans les systèmes afin de détecter toute altération des données traitées
BDM_SSA.3.1	L'authentification des messages doit être utilisée pour les applications pour lesquelles la protection du contenu des messages constitue une exigence de sécurité
BDM_SSA.4.1	Les données de sortie d'un système d'applications doivent être validées pour faire en sorte que le traitement des informations stockées soit correct et approprié aux circonstances

3.2.8.3 BDM_COC : Mesures cryptographiques (§10.3)

Code	Libellé
BDM_COC.1.1	Une politique sur l'utilisation des commandes cryptographiques pour la protection des informations doit être élaborée et suivie
BDM_COC.2.1	Un cryptage doit être appliqué pour protéger les informations confidentielles ou cruciales
BDM_COC.3.1	Des signatures numériques doivent être utilisées pour protéger l'authenticité et l'intégrité de l'information électronique
BDM_COC.4.1	Des services de non répudiation doivent être utilisés afin de régler des différends sur l'occurrence ou la non occurrence d'un événement ou d'une action
BDM_COC.5.1	Un système de gestion basé sur un ensemble convenu de normes, de procédures et de méthodes doit être utilisé afin de soutenir l'utilisation par l'organisme des deux types de techniques cryptographiques

3.2.8.4 BDM_SFS : Sécurité des fichiers (§10.4)

Code	Libellé
BDM_SFS.1.1	Une maîtrise doit être appliquée sur l'implantation de logiciels sur les systèmes opérationnels
BDM_SFS.2.1	Les données d'essai doivent être protégées et maîtrisées
BDM_SFS.3.1	Une maîtrise stricte doit être maintenue sur l'accès aux bibliothèques de programmes sources

3.2.8.5 BDM_SED : Sécurité des environnements de développement et de soutien (§10.5)

Code	Libellé
BDM_SED.1.1	L'application des modifications doit être maîtrisée de façon stricte en utilisant des procédures de maîtrise des modifications afin de minimiser l'altération des systèmes d'information
BDM_SED.2.1	Une revue et un essai des systèmes d'applications doivent être effectués lorsque des modifications sont apportées
BDM_SED.3.1	Il faut décourager d'apporter des modifications aux progiciels et les modifications essentielles doivent être maîtrisées de manière stricte
BDM_SED.4.1	L'achat, l'utilisation et la modification des logiciels doivent être maîtrisés et contrôlés afin de les protéger contre la possibilité d'introduction de voies secrètes et de code de Troie

Code	Libellé
BDM_SED.5.1	Des mesures de maîtrise doivent être appliquées afin de sécuriser le développement sous-traité de logiciels

3.2.9 BCA : Gestion de la continuité des activités de l'organisme (Chapitre 11)

3.2.9.1 BCA_AGC : Aspects de la gestion de la continuité des activités de l'organisme (§11.1)

Code	Libellé
BCA_AGC.1.1	Un processus géré doit être établi dans tout l'organisme pour le développement et le maintien de la continuité des activités professionnelles
BCA_AGC.2.1	Un plan stratégique basé sur une évaluation des risques appropriée, doit être élaboré afin de déterminer l'approche globale vis à vis de la continuité des activités professionnelles
BCA_AGC.3.1	Des plans doivent être élaborés afin de maintenir ou de rétablir les activités professionnelles dans les délais requis après une interruption ou une défaillance de processus professionnels cruciaux
BCA_AGC.4.1	Un seul cadre de planification de continuité des activités professionnelles doit être maintenu afin d'obtenir une cohérence de tous les plans et d'identifier les priorités en matière d'essais et de maintenance
BCA_AGC.5.1	Les plans de continuité des activités professionnelles doivent être essayés régulièrement et maintenus par des revues régulières afin de s'assurer qu'ils sont actualisés et efficaces

3.2.10 BCO : Conformité (Chapitre 12)

3.2.10.1 BCO_CEL : Conformité aux exigences légales (§12.1)

Code	Libellé
BCO_CEL.1.1	Toutes les exigences légales, réglementaires et contractuelles doivent être définies explicitement et documentées pour chaque système informatique
BCO_CEL.2.1	Des procédures appropriées doivent être appliquées afin d'assurer la conformité aux exigences légales sur l'utilisation de produits pour lesquels il pourrait y avoir des droits de propriété intellectuelle et sur l'utilisation de logiciels propriétaires
BCO_CEL.3.1	Les registres importants de l'organisme doivent être protégés contre toute perte, destruction et falsification
BCO_CEL.4.1	Des mesures de maîtrise doivent être appliquées afin de protéger les renseignements personnels conformément à la législation pertinente
BCO_CEL.5.1	La direction doit autoriser l'utilisation des infrastructures de traitement de l'information et des mesures de maîtrise doivent être appliquées pour empêcher l'utilisation abusive de ces infrastructures
BCO_CEL.6.1	Des mesures de maîtrise doivent être établies pour assurer la conformité aux conventions, aux lois, aux règlements nationaux ou aux autres instruments ayant pour but de maîtriser l'accès aux commandes cryptographiques ou leur utilisation
BCO_CEL.7.1	Lorsqu'une action contre une personne implique une poursuite civile ou criminelle, les preuves présentées doivent êtres conformes aux règles prescrites pour les preuves dans la loi pertinente ou dans les règlements du tribunal spécifique concerné
BCO_CEL.7.2	Lorsqu'une action contre une personne implique une poursuite civile ou criminelle, les preuves présentées doivent êtres conformes à toute norme ou à tout code de bonne pratique publié pour la production de preuves admissibles

3.2.10.2 BCO_RPS : Examens de la politique de sécurité et de la conformité technique (§12.2)

Code	Libellé
BCO_RPS.1.1	Les responsables doivent veiller à ce que toutes les procédures de sécurité dans leur secteur de responsabilité soient suivies correctement

Code	Libellé
BCO_RPS.1.2	Tous les secteurs au sein de l'organisme doivent être soumis à des revues régulières afin d'assurer leur conformité aux politiques et aux normes de sécurité
BCO_RPS.2.1	Les systèmes informatiques doivent être vérifiés régulièrement quant à leur conformité aux normes de mise en œuvre de la sécurité

3.2.10.3 BCO_CAS : Considérations sur les audits des systèmes (§12.3)

Code	Libellé
BCO_CAS.1.1	Les audits des systèmes opérationnels doivent être planifiés et approuvés de façon à minimiser les risques de perturbation des processus professionnels
BCO_CAS.2.1	L'accès aux outils d'audit des systèmes doit être protégé afin d'empêcher toute compromission ou toute utilisation abusive éventuelle

3.3 Autres exigences

3.3.1 CCS : Consigne de sécurité

3.3.1.1 CCS_SIN : Consignes en cas de sinistre

1- Support des consignes

Code	Libellé
CCS_SIN.1.1	Les consignes de sécurité en cas de sinistre doivent être rédigées de façon claire et lisible en respectant les normes et standards en usage
CCS_SIN.1.2	Les consignes de sécurité en cas de sinistre doivent être affichées à hauteur d'homme dans des endroits dégagés en respectant les normes et standards en usage
CCS_SIN.1.3	Les consignes de sécurité en cas de sinistre doivent être affichées en plusieurs endroits du site et notamment dans les endroits de passage et les endroits concernés par les consignes (ascenseur, installation susceptible de provoquer un dégât des eaux…)
CCS_SIN.1.4	Les consignes de sécurité en cas de sinistre doivent être imprimées sur un support qui attire l'œil

2- Contenu des consignes

Code	Libellé
CCS_SIN.2.1	La procédure d'appel des services de secours (pompiers, SAMU, police...) doit être clairement mentionnée sur les consignes de sécurité en cas de sinistre
CCS_SIN.2.2	La procédure d'évacuation du site (chemin d'évacuation, lieu de rassemblement…) doit être clairement mentionnée sur les consignes de sécurité consacrées aux sinistres nécessitant l'évacuation (incendie, pollution importante, attentat…)
CCS_SIN.2.3	Les consignes de sécurité doivent indiquer les actions adaptées à entreprendre (que faire quand on est pris dans la fumée, premiers secours à un électrocuté, mesures d'urgence en cas de dégât des eaux, protection des matériels en cas de sinistre…)

3- Gestion des consignes

Code	Libellé
CCS_SIN.3.1	Les consignes de sécurité en cas de sinistre doivent être régulièrement revues pour s'assurer qu'elles sont à jour (fréquence à définir mais en aucun cas supérieure à tous les 2 ans)
CCS_SIN.3.2	Le responsable de la revue des consignes de sécurité en cas de sinistre doit être clairement identifié
CCS_SIN.3.3	Les consignes de sécurité en cas de sinistre doivent être validées régulièrement par les services de secours en cas de sinistre (pompier, SAMU…)
CCS_SIN.3.4	Toute mise à jour des consignes de sécurité en cas de sinistre doit donner lieu à une communication à l'ensemble du personnel du site
CCS_SIN.3.5	Des sensibilisations aux consignes de sécurité et éventuellement des exercices pratiques (tests, exercices d'évacuation, simulation de sinistre) doivent être organisés régulièrement (fréquence à définir mais en aucun cas supérieure à tous les 2 ans)

3.3.1.2 CCS_CSP : Consignes de sécurité préventives

1- Support des consignes

Code	Libellé
CCS_CSP.1.1	Les consignes de sécurité préventives (interdiction de fumer près de matériaux inflammables par exemple) doivent être rédigées de façon claire et lisible

Code	Libellé
CCS_CSP.1.2	Les consignes de sécurité préventives doivent être affichées à hauteur d'homme dans des endroits dégagés
CCS_CSP.1.3	Les consignes de sécurité préventives doivent être affichées dans les endroits concernés par les consignes
CCS_CSP.1.4	Les consignes de sécurité préventives doivent être imprimées sur un support qui attire l'œil

2- Contenu des consignes

Code	Libellé
CCS_CSP.2.1	Les consignes de sécurité préventives doivent être régulièrement revues pour s'assurer qu'elles sont à jour (fréquence à définir mais en aucun cas supérieure à tous les 2 ans)
CCS_CSP.2.2	Le responsable de la revue des consignes de sécurité préventives doit être clairement identifié
CCS_CSP.2.3	Toute mise à jour des consignes de sécurité préventives doit donner lieu à une communication à l'ensemble du personnel du site
CCS_CSP.2.4	Les personnes extérieures doivent être informées des consignes de sécurité préventives par leur interlocuteur

3- Gestion des consignes

3.3.1.3 CCS_SSE : Consignes de sécurité pour les services essentiels

Code	Libellé
CCS_SSE.1.1	Les consignes de sécurité pour les services essentiels doivent être rédigées de façon claire et lisible
CCS_SSE.1.2	Les consignes de sécurité pour les services essentiels doivent présenter des mesures préventives pour éviter la perte des services essentiels (branchement des postes sur le courant ondulé par exemple)
CCS_SSE.1.3	Les consignes de sécurité pour les services essentiels doivent présenter les procédures d'alerte dans le cas d'incident (personne à contacter en cas de coupure de ligne télécom par exemple)
CCS_SSE.1.4	Les consignes de sécurité pour les services essentiels doivent présenter des mesures de réaction en cas d'incident (installation du climatiseur de dépannage par exemple)
CCS_SSE.1.5	Les consignes de sécurité pour les services essentiels doivent être revues régulièrement pour s'assurer qu'elles sont à jour
CCS_SSE.1.6	Le responsable de la revue des consignes de sécurité pour les services essentiels doit être clairement identifié
CCS_SSE.1.7	Toute mise à jour des consignes de sécurité pour les services essentiels doit donner lieu à une communication à l'ensemble du personnel du site

3.3.1.4 CCS_CSG : Consignes de sécurité générales

Code	Libellé
CCS_CSG.1.1	Des consignes de sécurité de bon usage des matériels et supports doivent être élaborées et diffusées à l'ensemble des utilisateurs potentiels
CCS_CSG.1.2	Les consignes de sécurité de bon usage doivent indiquer les pratiques qu'il convient d'éviter (interdiction de fumer, de manger ou de boire près d'un matériel, sensibilisation à la saturation des espaces de stockage ou des ressources de traitement…)
CCS_CSG.1.3	Les consignes de sécurité de bon usage doivent indiquer les mesures de prévention à mettre en œuvre (protection lors du transport, conditions de stockage…)
CCS_CSG.1.4	Les consignes de sécurité de bon usage doivent intégrer des règles sur l'environnement d'exploitation des infrastructures de traitement de l'information (température, hygrométrie…)

Code	Libellé
CCS_CSG.1.5	Les consignes de sécurité de bon usage doivent être revues régulièrement afin de s'assurer qu'elles sont à jour
CCS_CSG.1.6	Le responsable de la revue des consignes de sécurité de bon usage doit être clairement identifié
CCS_CSG.1.7	Toute mise à jour des consignes de sécurité de bon usage doit donner lieu à une communication à l'ensemble du personnel du site

3.3.1.5 CCS_CHI : Charte informatique

Code	Libellé
CCS_CHI.1.1	Les utilisateurs du système d'information (internes comme externes) doivent s'engager à respecter les consignes d'utilisation en signant une charte informatique basée sur les consignes de sécurité de bon usage

3.3.1.6 CCS_SRI : Partie sécurité du règlement intérieur

Code	Libellé
CCS_SRI.1.1	Les responsabilités sécurité en relation avec le système d'information doivent être rappelées dans le règlement intérieur

3.3.1.7 CCS_RGI : Règles générales d'installation

Code	Libellé
CCS_RGI.1.1	Des règles générales basées sur les recommandations des constructeurs et les besoins de sécurité identifiés doivent être établies pour l'installation des matériels

3.3.2 CRR : Risques résiduels

3.3.2.1 CRR_ETU : Étude des risques résiduels

1- Identification et évaluation

Code	Libellé
CRR_ETU.1.1	Une étude de risque doit être menée et régulièrement remise à jour afin de déterminer les risques couverts, les risques à couvrir et les risques résiduels
CRR_ETU.1.2	Les risques résiduels identifiés doivent être évalués en terme de faisabilité / probabilité ainsi qu'en terme d'impact (financier, métier, organisationnel, humain…)

2- Plan d'action en cas de réalisation

Code	Libellé
CRR_ETU.2.1	Un plan d'action doit être élaboré pour chaque risque résiduel afin de limiter le plus possible les impacts directs et d'éviter au maximum les impacts indirects et les effets de bord en cas de réalisation du risque
CRR_ETU.2.2	Dans les cas où cela est possible (existence de contrat d'assurance adapté, primes d'assurance maîtrisées...), les risques résiduels doivent être couvert par des assurances adaptées

3.3.2.2 CRR_SEN : Sensibilisation aux risques résiduels

Code	Libellé
CRR_SEN.1.1	Le personnel de l'organisation doit être sensibilisé aux risques résiduels et aux mesures prises pour réduire leur probabilité / faisabilité et leur impact
CRR_SEN.1.2	Le personnel de l'organisation doit être formé aux plans d'action en cas de réalisation de risque résiduel

3.3.3 CIS : Installation des sites

3.3.3.1 CIS_PSI : Chapitre de la PSI traitant de la sécurité physique

Code	Libellé

Code	Libellé
CIS_PSI.1.1	La politique de sécurité doit intégrer un chapitre concernant la sécurité physique des sites
CIS_PSI.1.2	Le chapitre concernant la sécurité physique des sites de la politique de sécurité doit identifier des normes d'installation de sites
CIS_PSI.1.3	Les normes d'installation de sites doivent comporter des mesures de protection et de réduction d'impact pour les sinistres

3.3.3.2 CIS_CSI : Consignes pour l'installation de sites

1- Gestion des consignes

Code	Libellé
CIS_CSI.1.1	Les normes d'installation de sites doivent être basées sur les normes et les standards nationaux et/ou internationaux en vigueur pour la protection contre les sinistres (incendie, accident…)
CIS_CSI.1.2	Les normes d'installation de sites doivent définir une nomenclature de zonage physique permettant de réduire les impacts des sinistres (isolation de zone par porte coupe-feu par exemple)
CIS_CSI.1.3	L'adéquation entre les normes d'installations de sites et les normes et standards nationaux et/ou internationaux en vigueur pour la protection contre les sinistres doit être validée régulièrement par les services de secours (pompiers, SAMU…)

2- Audit du respect des consignes

Code	Libellé
CIS_CSI.2.1	Les locaux (et en particulier ceux des sites vieillissant) doivent être régulièrement audités de conformité de manière à vérifier qu'ils respectent toujours les normes et standards d'installation
CIS_CSI.2.2	Les responsables de l'évaluation des sites et leurs remplaçants doivent être clairement identifiés
CIS_CSI.2.3	Les responsables de l'évaluation des sites et leurs remplaçants doivent être sensibilisés à la protection des sites et formés aux normes et standards d'installation
CIS_CSI.2.4	Les audits de conformité des sites doivent donner lieu à un compte rendu détaillé diffusé à la direction
CIS_CSI.2.5	Les comptes rendus d'audit de conformité des sites doivent être conservés, exploités et gérés comme les autres traces de sécurité du système d'information

3.3.3.3 CIS_CDL : Construction des locaux

Code	Libellé
CIS_CDL.1.1	Les risques majeurs inévitables (tempêtes, ouragan, tremblements de terre…) doivent être pris en compte lors de la construction et de l'aménagement des locaux

3.3.3.4 CIS_ADL : Aménagement des locaux

1- Ouvertures vers l'extérieur

Code	Libellé
CIS_ADL.1.1	En cas de vis à vis, les vitres des locaux doivent être teintées.
CIS_ADL.1.2	La présence de fenêtre sur la voie publique ne doit pas permettre un accès facile aux locaux (barreaux, vitres renforcées, impossibilité d'ouvrir complètement la fenêtre, alarme quand une fenêtre reste ouverte en dehors des heures d'ouverture du site…)

2- Conditions d'hébergement

Code	Libellé

Code	Libellé
CIS_ADL.2.1	L'aménagement des locaux doit tenir compte des éléments qu'il est prévu d'y installer (contrôle de la température, surveillance de l'hygrométrie, filtrage de poussières ou autres éléments polluants…)
CIS_ADL.2.2	Les équipements doivent être installés le plus loin possible des éléments susceptibles de les endommager (canalisations d'eau, source de rayonnement électromagnétique ou thermique…)
CIS_ADL.2.3	Les locaux techniques doivent être suffisamment spacieux pou permettre une organisation claire des installations et ne pas gêner l'exploitation du matériel

3- Identification des installations

Code	Libellé
CIS_ADL.3.1	Les installations standards (câbles réseau, vanne de coupure d'eau, fusibles...) doivent être identifiées de manière à en connaître la localisation et le rôle

3.3.3.5 CIS_SSI : Sélection du site d'implantation

Code	Libellé
CIS_SSI.1.1	La proximité de services d'urgence doit être un critère dans la sélection de l'implantation du site
CIS_SSI.1.2	La sélection de l'implantation d'un site doit tenir compte des risques inhérent au lieu d'implantation (zone inondable, proximité d'une implantation industrielle à risque, pollution…)
CIS_SSI.1.3	La sélection de l'implantation du site doit tenir compte des possibilités de destruction causée par un événement extérieur (collisions, attentats…)
CIS_SSI.1.4	La sélection de l'implantation du site doit tenir compte des risques d'atteinte à la disponibilité du personnel (site peu desservi par les transports, site aisé à bloquer…)

3.3.3.6 CIS_MPP : Mesures de protection

1- Protection générale

Code	Libellé
CIS_MPP.1.1	Les alimentations en services essentiels doivent être muni de dispositifs de coupure (dont un dispositif de coupure générale) identifiés et accessibles
CIS_MPP.1.2	Les dispositifs de coupure des alimentations en services essentiels ainsi que tout élément permettant susceptible de permettre un arrêt des services essentiels doivent être protégés contre les accès non autorisés
CIS_MPP.1.3	Les éléments susceptibles de permettre un arrêt des services essentiels doivent si possible être implantés sur le site

2- Protection incendie

Code	Libellé
CIS_MPP.2.1	Les locaux doivent être équipés de dispositifs de détection et de lutte anti-incendie
CIS_MPP.2.2	Les dispositifs de détection et de lutte anti-incendie doivent être adaptés aux sites et zones d'implantation et dimensionné de façon adéquate

3- Protection contre les dégâts des eaux

Code	Libellé
CIS_MPP.3.1	Les sites susceptibles de subir des dégâts des eaux importants doivent être équipés de dispositifs d'évacuation en conséquence (puisard, pompe…)
CIS_MPP.3.2	Les zones particulièrement sensibles aux dégâts des eaux (équipements électriques, archive papier…) doivent être équipées de détecteurs adaptés
CIS_MPP.3.3	Les points de contacts avec l'extérieur (plafonds, fenêtres…) doivent résister à l'eau et leur étanchéité doit être vérifiée régulièrement
CIS_MPP.3.4	Des protections spécifiques contre la montée des eaux doivent être prévues pour les sites en zone inondable

3.3.3.7 CIS_ZOS : Zones de sécurité

Code	Libellé
CIS_ZOS.1.1	Les organismes doivent utiliser des périmètres de sécurité pour protéger les zones qui contiennent des équipements de production ou de distribution des services essentiels

3.3.4 CRI : Relations inter-sites

3.3.4.1 CRI_MOF : Maîtrise des organisations filles

1- Généralité

Code	Libellé
CRI_MOF.1.1	Les sites appartenant à l'organisme doivent s'engager à respecter les dispositions de la politique de sécurité

2- Installation initiale

Code	Libellé
CRI_MOF.2.1	Les modifications importantes dans un site appartenant à l'organisme doivent donner lieu à un rapport d'installation à destination du responsable de la sécurité de l'organisme (installation initiale du site, modification du raccordement réseau…)

3.3.5 CET : Encadrement des tiers (ex AEV)

3.3.5.1 CET_EGT : Encadrement général des tiers

1- Arrivée sur le site

Code	Libellé
CET_EGT.1.1	Les personnes extérieures ne doivent pas pouvoir pénétrer sur le site ou en sortir sans passer par l'accueil
CET_EGT.1.2	Dans la mesure du possible, chaque visite de tiers doit être annoncée et le personnel de l'accueil doit avoir la liste des noms de tous les visiteurs prévus par jour avec l'heure prévue d'arrivée et l'interlocuteur interne concerné
CET_EGT.1.3	Chaque visiteur doit être authentifié à son arrivée par une pièce d'identité officielle; un badge visiteur doit lui être fourni en échange de sa pièce d'identité
CET_EGT.1.4	Si la visite était prévue, le nom de chaque visiteur doit être validé avec la liste des visiteurs prévus pour la journée. Les noms non présents sur la liste doivent y être ajoutés
CET_EGT.1.5	L'heure d'arrivée et l'heure de départ de chaque visiteur doit être notée
CET_EGT.1.6	Le nom, l'heure d'arrivée, l'heure de départ et l'interlocuteur interne de chaque visiteur doivent être conservés, exploités et gérés comme les autres traces de sécurité du système d'information
CET_EGT.1.7	Un interlocuteur interne doit être attribué à tout visiteur d'une visite non prévue et le visiteur ne doit pas être autorisé à pénétrer dans les locaux sans être accompagné par son interlocuteur interne
CET_EGT.1.8	Si un tiers apporte du matériel ou des supports dans les locaux, une liste précise du matériel doit être dressée et conservée avec la carte d'identité du tiers et dans la mesure du possible, le matériel doit être marqué comme matériel extérieur
CET_EGT.1.9	Un tiers ayant apporté du matériel ou des supports doit sortir des locaux avec le même matériel ou un récépissé signé par matériel en plus ou en moins
CET_EGT.1.10	Les récépissés de réception ou de livraison de matériel ou de supports doivent être déposés en main propre à l'accueil par l'interlocuteur interne au moment du départ du tiers concerné

2- Présence dans les locaux

Code	Libellé

Code	Libellé
CET_EGT.2.1	L'interlocuteur interne d'un visiteur doit être contacté dès l'arrivée du visiteur
CET_EGT.2.2	L'interlocuteur interne d'un visiteur prendre en charge le visiteur à partir de l'accueil
CET_EGT.2.3	A partir de sa prise en charge, l'interlocuteur interne est responsable d'un visiteur jusqu'à son départ. Il doit notamment s'assurer que la visite se déroule en accord avec les principes de sécurité énoncés dans la politique de sécurité

3- Vérification des habilitations (porte aussi sur les employés)

Code	Libellé
CET_EGT.3.1	Les accès à un site ou à une zone avec des besoins de sécurité spécifiques doivent faire l'objet d'une validation de l'habilitation des visiteurs
CET_EGT.3.2	Dans le cas d'un visiteur externe, le responsable interne du visiteur doit être habilité de façon adéquate
CET_EGT.3.3	Dans le cas d'un accès par un employé de l'organisme, son habilitation doit être vérifiée au niveau de l'accueil du site ou de la zone
CET_EGT.3.4	La validation des habilitations peut être effectuée par une interrogation manuelle de la base des habilitations une fois l'authentification par pièce d'identité effectuée ou par une solution d'authentification automatique (ex: à base de badges personnels)
CET_EGT.3.5	Dans le cas d'une vérification des habilitations automatique, les données d'identification ainsi que la date et l'heure de l'entrée doivent être conservées, exploitées et gérées comme les autres traces de sécurité du système d'information

3.3.5.2 CET_EIP : Encadrement des intervenants ponctuels

1- Intervention

Code	Libellé
CET_EIP.1.1	Tout intervenant sur le système d'information doit être informé avant le début de son intervention des consignes de sécurité
CET_EIP.1.2	L'interlocuteur interne d'un intervenant est responsable de toutes les actions d'un intervenant pendant la durée de l'intervention (intervention technique, respect des consignes et de la politique de sécurité notamment pour la protection des informations)
CET_EIP.1.3	Une intervention doit être clôturée par une recette d'intervention permettant de contrôler les opérations effectuées et les résultats obtenus
CET_EIP.1.4	Le procès verbal de recette d'intervention doit préciser le nom de l'intervenant, son entreprise, le jour et les horaires de l'intervention, les opérations effectuées, les résultats obtenus, les problèmes éventuels et le nom de l'interlocuteur interne
CET_EIP.1.5	Le procès verbal de recette d'intervention doit être signé par le ou les intervenants, par l'interlocuteur interne et par le responsable de la recette d'intervention s'il est différent de l'interlocuteur interne
CET_EIP.1.6	Les procès verbaux de recette d'intervention doivent être conservés, exploités et gérés comme les autres traces de sécurité du système d'information

3.3.5.3 CET_PLD : Encadrement des prestations de longue durée sur site

1- Lancement de la prestation

Code	Libellé
CET_PLD.1.1	Une fois la procédure d'accueil initiale effectuée, un prestataire sur site doit pouvoir être traité comme un personnel temporaire de l'organisation (badge d'accès, droits d'accès au système d'information selon les besoins de la prestation…)
CET_PLD.1.2	Tout élément fourni à un prestataire sur site dans le cadre de sa mission (badge d'accès, identifiant et mot de passe de connexion…) doit être identifié et répertorié sur une liste des éléments fournis au prestataire avec la date de la mise à disposition
CET_PLD.1.3	La liste des éléments fournis à un prestataire sur site doit être conservée, exploitée et gérée comme les autres traces de sécurité du système d'information

Code	Libellé
CET_PLD.1.4	Les consignes de sécurité et la politique de sécurité doivent être fournies à chaque prestataire sur site au début de la prestation
CET_PLD.1.5	Avant le début de sa prestation, un prestataire sur site doit s'engager à respecter les consignes de sécurité et les dispositions de la politique de sécurité
CET_PLD.1.6	Avant le début de sa prestation, un prestataire sur site doit signer un engagement officiel de confidentialité

2- Fin de la prestation

Code	Libellé
CET_PLD.2.1	A la fin de sa prestation, un prestataire sur site doit restituer tous les éléments physiques (badge d'accès par exemple) qui lui ont été fournis dans le cadre de sa mission
CET_PLD.2.2	La restitution des éléments fournis à un prestataire sur site doit faire l'objet d'un procès verbal de restitution daté et signé par le prestataire et par un responsable de l'organisation
CET_PLD.2.3	A la fin d'une prestation sur site, tous les éléments logiques (identifiant et mot de passe de connexion par exemple) attribués à un prestataire dans le cadre de sa mission doivent être désactivés ou détruits
CET_PLD.2.4	La désactivation ou la destruction des éléments logiques attribués à un prestataire dans le cadre de sa mission doit faire l'objet d'un procès verbal de désactivation ou de destruction daté et signé par le responsable de l'opération
CET_PLD.2.5	Les procès verbaux de fin de prestation doivent être conservés, exploités et gérées comme les autres traces de sécurité du système d'information

3.3.6 CAR : Administration réseau

3.3.6.1 CAR_PAR : Protection de l'administration réseau

Code	Libellé
CAR_PAR.1.1	Les logiciels d'administration ne doivent pas être sensibles aux dénis de service

3.3.6.2 CAR_AAR : Attribution de l'administration réseau

Code	Libellé
CAR_AAR.1.1	L'administration des machines doit permettre de détecter les consommations excessives de ressources

3.3.7 CGS : Gestion de la sécurité

3.3.7.1 CGS_GMP : Gestion des mots de passe

Code	Libellé
CGS_GMP.1.1	La politique de mot de passe doit imposer un changement périodique
CGS_GMP.1.2	Les saisies de mots de passe doivent être faites à l'abri des regards indiscrets
CGS_GMP.1.3	Les utilisateurs doivent être sensibilisés sur les bonnes pratiques sécurité lors de la sélection et de l'utilisation des mots de passes

3.3.7.2 CGS_SVG : Sauvegarde

1- Procédure de sauvegarde

Code	Libellé
CGS_SVG.1.1	La politique de sécurité doit inclure une politique de sauvegarde
CGS_SVG.1.2	L'ensemble des documents électroniques doit être pris en compte dans la politique de sauvegarde
CGS_SVG.1.3	Les données devant faire l'objet d'une sauvegarde doivent être identifiées dans des procédures de sauvegarde spécifiques

Code	Libellé
CGS_SVG.1.4	Les procédures de sauvegarde doivent indiquer les modalités de sauvegarde, les supports à utiliser, la fréquence des sauvegardes ainsi que les procédures de gestion des supports vierges et une fois les sauvegardes réalisées
CGS_SVG.1.5	Les responsables de chaque opération de sauvegarde ainsi que leurs remplaçants doivent être clairement identifiés
CGS_SVG.1.6	Les responsables des sauvegardes et leurs remplaçants doivent être formés aux opérations de sauvegarde
CGS_SVG.1.7	La politique de sauvegarde doit être revue régulièrement de manière à l'adapter aux évolutions du système d'information en conservant une prise en compte des anciennes sauvegardes
CGS_SVG.1.8	Les responsables de la revue des procédures de sauvegarde doivent être clairement identifiés
CGS_SVG.1.9	Toute modification d'une procédure de sauvegarde doit être communiquée aux responsables des sauvegardes concernés ainsi qu'à leurs remplaçants

2- Protection des sauvegardes

Code	Libellé
CGS_SVG.2.1	Les sauvegardes doivent bénéficier du même niveau de protection que les données sauvegardées

3.3.7.3 CGS_ARC : Archivage

1- Procédure d'archivage

Code	Libellé
CGS_ARC.1.1	L'ensemble des données devant être archivée doit faire l'objet d'une expression de besoins en terme de délai de rétention et de fiabilité des supports
CGS_ARC.1.2	Les mesures de conservation des données à archiver doivent être conformes aux besoins exprimés pour l'archivage des données concernées
CGS_ARC.1.3	Les données devant faire l'objet d'un archivage doivent être identifiées dans des procédures d'archivage spécifiques
CGS_ARC.1.4	Les procédures d'archivage doivent indiquer les modalités d'archivage des données, les supports à utiliser, la fréquence des archivages ainsi que les procédures de gestion des supports d'archivage vierges et une fois les opérations d'archivage réalisées
CGS_ARC.1.5	Les responsables de chaque opération d'archivage ainsi que leurs remplaçants doivent être clairement identifiés
CGS_ARC.1.6	Les responsables de l'archivage et leurs remplaçants doivent être formés aux opérations d'archivage
CGS_ARC.1.7	Les procédures d'archivage doivent être régulièrement revues de manière à l'adapter aux éventuelles évolutions des besoins d'archivage des données en conservant une prise en compte des anciennes archives
CGS_ARC.1.8	Les responsables de la revue des procédures d'archivage doivent être clairement identifiés
CGS_ARC.1.9	Toute modification d'une procédure d'archivage doit être communiquée aux responsables d'archivage concernés ainsi qu'à leurs remplaçants

2- Protection des archives

Code	Libellé
CGS_ARC.2.1	Les archives doivent bénéficier du même niveau de protection que les données archivées

3.3.7.4 CGS_PPS : Protection des postes

1- Protection systèmes

Code	Libellé

Code	Libellé
CGS_PPS.1.1	Les protections du Bios contre les démarrages sur des supports amovibles doivent être activées
CGS_PPS.1.2	Les services, fonctions et interfaces informatiques qui ne sont pas utilisés doivent être désactivés
CGS_PPS.1.3	Les services, fonctions et interfaces qui ne sont utilisés que ponctuellement doivent être désactivés quand ils ne sont pas utilisés

2- Protection des logiciels installés

Code	Libellé
CGS_PPS.2.1	Seul le personnel autorisé doit être en mesure de modifier le système ou les logiciels installés
CGS_PPS.2.2	La configuration des logiciels doit prendre en compte l'aspect sécurité
CGS_PPS.2.3	Les logiciels utilisés doivent être communément employés ou avoir été audité
CGS_PPS.2.4	Les logiciels utilisés doivent être exempts de failles de sécurité connues
CGS_PPS.2.5	L'intégrité des codes doit être protégée contre les modifications non autorisées

3- Protection physique des matériels

Code	Libellé
CGS_PPS.3.1	Les matériels doivent être protégés contre le vol (câble anti-vol, gravage…)
CGS_PPS.3.2	Les supports amovibles doivent être inventoriés et protégés contre le vol et les accès non autorisés (stockage dans une armoire fermée dont seuls les personnes habilité ont la clé, restriction d'accès pour les locaux d'utilisation…)

3.3.7.5 CGS_GLI : Gestion des licences

1- Gestion des licences

Code	Libellé
CGS_GLI.1.1	Un dispositif opérationnel de gestion de licence doit être mis en en place
CGS_GLI.1.2	Les numéros des licences doivent être sauvegardés séparément
CGS_GLI.1.3	Les contrats de licence doivent être conservés à l'abris du feu et des autres sinistres susceptibles de les rendre inutilisables
CGS_GLI.1.4	L'accès aux licences doit être retreint aux personnes autorisées

2- Gestion des logiciels soumis à des licences

Code	Libellé
CGS_GLI.2.1	L'accès aux versions installables des logicielles doit être retreint aux personnes autorisées

3.3.7.6 CGS_OML : Garantie d'origine matériel et logiciel

Code	Libellé
CGS_OML.1.1	L'origine des installations, matériels ou logiciels et de leurs mises à jour doit pouvoir être garantie
CGS_OML.1.2	Les certifications éventuelles des installations, matériels ou logiciels et de leurs mises à jour doivent être contrôlées
CGS_OML.1.3	Des mesures doivent être prises pour garantir l'authenticité des codes

3.3.7.7 CGS_GMA : Gestion de la maintenance

1- Dispositions générales

Code	Libellé
CGS_GMA.1.1	Les installations, les matériels et les logiciels du système d'information ainsi que ceux qui assurent la protection du système d'information et la fourniture des services essentiels doivent être maintenus et testés régulièrement

Code	Libellé
CGS_GMA.1.2	Les maintenances et tests de bon fonctionnement des éléments du système d'information, des éléments de sécurité et des éléments fournissant les services essentiels doivent suivre les recommandations des constructeurs et les normes et standards en vigueur

2- Maintenance interne

Code	Libellé
CGS_GMA.2.1	Dans le cas d'une maintenance interne, les responsables de la maintenance et leurs remplaçants doivent être formés aux opérations de maintenance sur les installations, matériels et/ou logiciels dont ils ont la charge
CGS_GMA.2.2	Dans le cas d'une maintenance interne, les documentations techniques des installations, matériels et/ou logiciels à maintenir doivent être à disposition des responsables de la maintenance et être accessibles aux remplaçants

3- Maintenance externe

Code	Libellé
CGS_GMA.3.1	Dans le cas d'une maintenance externe, un responsable du suivi de maintenance doit être désigné pour chaque élément (installation, matériel, logiciel…)
CGS_GMA.3.2	Dans le cas d'une maintenance externe, le responsable du suivi de maintenance doit s'assurer que les opérations de maintenance sont réalisées selon les fréquences prévues dans les contrats
CGS_GMA.3.3	Dans le cas d'une maintenance externe, le responsable du suivi de maintenance doit s'assurer qu'un contrat de maintenance adéquat est en permanence en cours pour chaque élément dont il a la charge (reconduction ou signature de nouveaux contrats)

4- Protection des accès à la maintenance

Code	Libellé
CGS_GMA.4.1	Les moyens de maintenance des systèmes et de matériels doivent bénéficier du même niveau de protection que les systèmes et matériels concernés

5- Budget de la maintenance

Code	Libellé
CGS_GMA.5.1	Le budget alloué à la maintenance doit être suffisant pour assurer une maintenance de qualité de tous les matériels et logiciels du système d'information

6- Maintenance évolutive

Code	Libellé
CGS_GMA.6.1	Les opérations de maintenance évolutives doivent toujours prévoir une procédure de retour arrière en cas d'anomalie lors d'une modification

3.3.7.8 CGS_GSU : Gestion du support

1- Dispositions générales

Code	Libellé
CGS_GSU.1.1	Un support doit être disponible pour les installations, les matériels et les logiciels du système d'information ainsi que ceux qui assurent la protection du système d'information
CGS_GSU.1.2	La procédure d'intervention du support doit être connue soit des utilisateurs du système d'information, soit au minimum des filières de gestion des incidents correspondantes
CGS_GSU.1.3	Dans le cas où des employés sont amenés utiliser le système d'information de l'organisme en dehors des locaux, le support doit être accessible depuis l'extérieur de l'organisme et le cas échéant depuis des pays en fort décalage horaire

2- Support interne

Code	Libellé
CGS_GSU.2.1	Dans le cas d'un support interne, les responsables du support et leurs remplaçants doivent être avoir bénéficié d'une formation approfondie sur les installations, matériels et/ou logiciels dont ils ont la charge
CGS_GSU.2.2	Dans le cas d'un support interne, les documentations techniques des installations, matériels et/ou logiciels concernées doivent être à disposition des responsables du support et être accessibles aux remplaçants
CGS_GSU.2.3	Dans le cas d'un support interne sur des éléments simples, le support peut être mutualisé avec la filière de gestion des incidents correspondante

3- Support externe

Code	Libellé
CGS_GSU.3.1	Dans le cas d'un support externe, un responsable du suivi de support doit être désigné pour chaque élément (installation, matériel, logiciel…) au sein de la filière de gestion des incidents correspondante
CGS_GSU.3.2	Dans le cas d'un support externe, le responsable du suivi de support est responsable du contact du support externe selon les modalités définies dans le contrat de support
CGS_GSU.3.3	Dans le cas d'un support externe, le responsable du suivi de support doit s'assurer qu'un contrat de support adéquat est en permanence en cours pour chaque élément dont il a la charge (reconduction ou signature de nouveaux contrats)

3.3.7.9 CGS_GDH : Gestion des habilitations

1- Définition des habilitations

Code	Libellé
CGS_GDH.1.1	Les utilisateurs doivent être habilités à consulter et/ou modifier les données ou les éléments du système d'information en fonction de leur besoin d'en connaître ou d'en modifier et non en fonction de leur position hiérarchique
CGS_GDH.1.2	Une procédure d'habilitation des utilisateurs doit être élaborée pour permettre la validation du besoin d'en connaître ou d'en modifier de chaque utilisateur avant son habilitation
CGS_GDH.1.3	La procédure d'habilitation doit être la plus légère et la plus complète possible de manière à ne pas gêner l'accès justifié aux données et ainsi de ne pas favoriser le prêt de droit d'accès
CGS_GDH.1.4	Les différents types d'habilitations doivent être directement liés aux besoins de sécurité identifiés pour les infrastructures et les informations
CGS_GDH.1.5	Les responsables de l'attribution des habilitations doivent être clairement identifiés en fonction des éléments sur lesquels portent les habilitations
CGS_GDH.1.6	Les types d'habilitations et les habilitations accordées doivent être régulièrement revues afin de s'assurer de leur adéquation avec les besoins du système d'information
CGS_GDH.1.7	La responsabilité de la révision des habilitations ne doit pas échoir aux responsables de l'attribution des habilitations
CGS_GDH.1.8	Une fois traités, les dossiers d'habilitation (identification de l'utilisateur demandeur, habilitations attribuées…) doivent être datés et archivés
CGS_GDH.1.9	Les dossiers d'habilitation archivés doivent être considérés et protégés comme des informations sensibles

2- Attributions liées aux habilitations

Code	Libellé
CGS_GDH.2.1	Les attributions associées à chaque habilitation doivent être clairement définies
CGS_GDH.2.2	Dès qu'un utilisateur obtient une habilitation, il doit être informé des attributions associées

3.3.7.10 CGS_PDI : Protection des infrastructures

Code	Libellé
CGS_PDI.1.1	La politique de sécurité doit lister les types de disposition à mettre en place afin de protéger les infrastructures de traitement de l'information

3.3.7.11 CGS_CIR : Classification de l'information et responsabilité

Code	Libellé
CGS_CIR.1.1	Les types de classification de l'information utilisés pour l'organisme doivent être décrits dans la politique de sécurité
CGS_CIR.1.2	Les dispositions de sécurité associées à chaque type de classification doivent être décrites dans la politique de sécurité
CGS_CIR.1.3	Les responsabilités de l'application des dispositions de sécurité associées à chaque type de classification en fonction de l'utilisation qui est faite des données doivent être décrite dans la politique de sécurité

3.3.7.12 CGS_PAI : Privilège d'accès à l'information

1- Définition des privilèges

Code	Libellé
CGS_PAI.1.1	Les responsables de la définition, de la mise en œuvre et du contrôle d'accès à l'information doivent être clairement identifiés
CGS_PAI.1.2	Les contrôles d'accès à l'information doivent être revus régulièrement de manière à vérifier leur adéquation avec les besoins de sécurité
CGS_PAI.1.3	Toute modification des contrôles d'accès à l'information doit faire l'objet d'une communication à l'ensemble des utilisateurs potentiels des systèmes concernés
CGS_PAI.1.4	La procédure de gestion des privilèges d'accès doit être la plus légère et la plus complète possible de manière à ne pas gêner l'accès aux données et ainsi de ne pas favoriser le prêt de moyen d'accès

2- Définition des droits sur lesquels se basent les privilèges

Code	Libellé
CGS_PAI.2.1	L'ensemble des droits attribuables doit être défini dans un règlement spécifique
CGS_PAI.2.2	Le règlement définissant les droits doit donner une définition clair des droits utilisés, notamment le droit d'en connaître et le droit d'en modifier
CGS_PAI.2.3	Le règlement définissant les droits doit donner des indications d'utilisation de ces droits en terme de contrôle d'accès et en terme d'habilitation

3.3.7.13 CGS_REC : Recette

Code	Libellé
CGS_REC.1.1	Les recettes et tests de bon fonctionnement des logiciels doivent être effectués sur l'ensemble des plates-formes sur lesquelles ils sont susceptibles d'être installés

3.3.7.14 CGS_GPC : Gestion des processus critiques

1- Localisation des processus critiques

Code	Libellé
CGS_GPC.1.1	Dans la mesure du possible, les processus critiques doivent être concentrés au niveau de l'organisme central
CGS_GPC.1.2	Si un processus critique doit être délocalisé hors de l'organisme central, des mesures de contrôle du processus par l'organisme central doivent être mises en place (rapport d'activité, administration distante…)

2- Contrôle des processus critiques

Code	Libellé
CGS_GPC.2.1	Les processus critiques ne doivent pas pouvoir être exécutés par une seule personne
CGS_GPC.2.2	Les résultats des processus critiques doivent être validés avant utilisation

Code	Libellé
CGS_GPC.2.3	La validation des processus critiques doit être effectuée par au moins deux responsables de l'organisme
CGS_GPC.2.4	Les responsables de la validation des processus critiques et leur remplaçants doivent être clairement identifiés

3.3.7.15 CGS_PEP : Protection des espaces partagés

Code	Libellé
CGS_PEP.1.1	Les espaces dédiés au partage ou à l'échange d'information doivent être protégés au même titre que les autres espaces du système d'information contre les accès non autorisés (habilitation, droit d'accès, authentification…)

3.3.7.16 CGS_OES : Organisation et sécurité

Code	Libellé
CGS_OES.1.1	L'organisation mise en place dans l'organisme et entre l'organisme et ses partenaires doit favoriser l'identification individuelle des utilisateurs
CGS_OES.1.2	Les changements éventuels d'organisation suite à un changement de politique ou de stratégie d'organisation ne doivent pas réduire le périmètre des risques couverts
CGS_OES.1.3	Les périodes de transition lors de changement d'organisation doivent être planifiées et ne pas permettre de recouvrement de droits d'accès et d'attribution

3.3.7.17 CGS_HSI : Protection de sécurité hors système d'information

Code	Libellé
CGS_HSI.1.1	Les équipements de sécurité ne faisant pas partie du système d'information (détecteur de fumée, mécanisme de détection des dégâts des eaux, paratonnerre...) doivent être protégés au même titre que les équipements du système d'information
CGS_HSI.1.2	Le personnel de l'organisation doit être sensibilisé à la protection des équipements de sécurité ne faisant pas partie du système d'information

3.3.7.18 CGS_GSS : Gestion des systèmes de secours

1- Dimensionnement

Code	Libellé
CGS_GSS.1.1	Les mécanismes de secours doivent au moins consister en des équipements redondants suffisamment dimensionnés pour assurer de façon satisfaisante les services identifiés comme stratégiques
CGS_GSS.1.2	Le dimensionnement des équipements redondants de secours doit être revu régulièrement et à chaque évolution majeure du système d'information afin de s'assurer qu'il est encore adapté
CGS_GSS.1.3	L'ensemble des secours (redondant ou non) doit être dimensionné de manière à fournir une qualité de service correspondant aux objectifs identifiés pour les solutions dégradées de secours
CGS_GSS.1.4	Dans la mesure du possible, les secours ne doivent pas être utilisés en fonctionnement nominal, dans le cas contraire, leur dimensionnement doit tenir compte de l'augmentation prévisible des besoins en ressources en cas d'incident

2- Déclenchement du secours

Code	Libellé
CGS_GSS.2.1	L'activation des équipements redondants de secours doit si possible être automatique
CGS_GSS.2.2	En cas de secours non activé automatiquement, le traitement d'un incident provoquant un arrêt de service doit débuter par l'activation la plus rapide possible du secours adéquat

3- Utilisation du secours

3.3.7.19 CGS_GMR : Gestion des mises au rebut

Code	Libellé
CGS_GMR.1.1	Les supports contenant des informations internes à l'organisme doivent être mis au rebut de manière à ne pas être accessible du public
CGS_GMR.1.2	Les supports contenant des informations confidentielles ne doivent pas être mis au rebus de manière à ne pas être accessible par une personne non autorisée

3.3.7.20 CGS_GDA : Gestion des authentifications

1- Généralité

Code	Libellé
CGS_GDA.1.1	L'authentification doit être obligatoire à partir d'un certain niveau de sécurité que ce soit pour la consultation ou la modification
CGS_GDA.1.2	Lorsque cela est applicable, l'authentification doit déboucher sur la consultation des privilèges de la personne ou de l'application authentifiée
CGS_GDA.1.3	Les accès aux systèmes doivent être journalisées avec si possible et au minimum l'identité de l'utilisateur, le système concerné et la date et l'heure de l'accès
CGS_GDA.1.4	Les opérations issues de l'exploitation des dispositifs d'accès doivent être tracées et journalisées au même titre que les accès aux systèmes

2- Authentification des personnes

Code	Libellé
CGS_GDA.2.1	L'authentification d'une personne doit obligatoirement être basée sur une donnée qu'elle connaît (mot de passe, pin code…) et éventuellement sur un objet qu'elle possède (badge, carte à puce…) ou sur une caractéristique physique (biométrie) voire les deux

3- Authentification des applications

Code	Libellé
CGS_GDA.3.1	L'authentification d'une application doit être basée sur un système garantissant qu'il n'y a pas d'usurpation d'application (certificat de signature par exemple)
CGS_GDA.3.2	Certaines fonctions sensibles (à définir) doivent automatiquement faire l'objet d'une authentification

3.3.7.21 CGS_CSR : Configuration des services réseaux

Code	Libellé
CGS_CSR.1.1	L'ensemble des services réseaux doit être configuré de manière à ne pas pouvoir être utilisé pour d'autres fonctionnalités que celles prévues
CGS_CSR.1.2	Les connexions doivent être filtrées de manière à ne pas permettre le trafic non prévu (exploitation de fonctionnement asynchrone, accès sur des ports non autorisés, spam…)
CGS_CSR.1.3	Le dispositif d'accès doit permettre de limiter les possibilités d'opérations illicites ou frauduleuses

3.3.7.22 CGS_CME : Configuration de la messagerie électronique

Code	Libellé
CGS_CME.1.1	La configuration de la messagerie électronique doit permettre de maîtriser les flux réseaux générés (réduction des émissions automatiques, listes de diffusion accessibles à tous…)

3.3.7.23 CGS_SUP : Supervision

Code	Libellé
CGS_SUP.1.1	La supervision des systèmes doit être la plus simple et la plus ergonomique possible (clarté des informations, outil adapté et unique permettant une supervision centrale…)

3.3.7.24 CGS_GDT : Gestion des traces

Code	Libellé
CGS_GDT.1.1	Les traces doivent au moins bénéficier du même niveau de protection que les opérations sur lesquelles elles portent et éventuellement d'un niveau plus élevé si elles comportent des données nominatives

3.3.8 CDO : Documentation

3.3.8.1 CDO_APP : Documentation sur les applications

Code	Libellé
CDO_APP.1.1	Les manuels de maintenance, d'exploitation et d'utilisation des applications ainsi que les éventuelles documentations internes complémentaires sur le sujet doivent être accessibles aux acteurs concernés
CDO_APP.1.2	Les procédures de maintenance, d'exploitation et d'utilisations des applications doivent être accessibles aux acteurs concernés
CDO_APP.1.3	Les documentations internes doivent être régulièrement remises à jour

3.3.8.2 CDO_SDC : Suivi des configurations

Code	Libellé
CDO_SDC.1.1	Un inventaire à jour des systèmes et de leur configuration doit être élaboré, mis à jour à chaque modification des systèmes ou des configurations et diffusé aux acteurs ayant besoin d'en connaître (mainteneur, développeur, support interne…)
CDO_SDC.1.2	Toute modification des configurations matérielles ou logicielles doit prendre en compte la compatibilité avec le reste du système d'information et les anciennes sauvegardes ou archives et prévoir une procédure de retour arrière en cas d'anomalie

3.3.9 CGI : Gestion des incidents

3.3.9.1 CGI_GDC : Gestion de crise

1- Détection d'une crise

Code	Libellé
CGI_GDC.1.1	Les situations de crise potentielles doivent être identifiées
CGI_GDC.1.2	Des seuils d'alerte de crise doivent être définis pour chaque crise potentielle identifiée de manière à savoir quand un organisme ou un site entre dans une situation de crise
CGI_GDC.1.3	Une métrique spécifique doit être élaborer pour permettre de détecter le passage des seuils d'alerte
CGI_GDC.1.4	Des remontés d'alerte automatiques doivent être mise en place de manière à déclencher la procédure de gestion de crise dès qu'un seuil d'alerte est atteint

2- Procédure de gestion de crise

Code	Libellé
CGI_GDC.2.1	La procédure de gestion de crise doit être automatiquement déclenchée dès qu'un seuil d'alerte est atteint
CGI_GDC.2.2	La procédure de gestion de crise peut être déclenchée manuellement par le dernier échelon d'escalade de gestion d'incident en dehors de l'atteinte d'un seuil d'alerte
CGI_GDC.2.3	En cas d'absence du dernier échelon d'escalade, la responsabilité du déclenchement manuel de la procédure de gestion de crise doit être transférée à une personne présente (remplaçant du dernier échelon d'escalade ou personne identifiée spécifiquement)
CGI_GDC.2.4	La chaîne de transfert de responsabilité du déclenchement manuel de la procédure de gestion de crise doit être clairement identifiée de manière à ce qu'il y ait toujours un responsable même en cas d'indisponibilité de plusieurs personnes

Code	Libellé
CGI_GDC.2.5	Les personnes susceptibles de déclencher manuellement la procédure de gestion du crise doivent être sensibilisées et formées au déclenchement manuel
CGI_GDC.2.6	Le déclenchement de la procédure de gestion de crise doit au minimum consister en un contact rapide du membre responsable de la cellule de crise correspondant à la situation

3- Composition de cellules de crise

Code	Libellé
CGI_GDC.3.1	Des cellules de crise doivent être constituées pour chaque type de crises potentielles (accident physique, attaque réseau, procédure légale…)
CGI_GDC.3.2	Une cellule de crise doit au minimum être composée d'un spécialiste du domaine et d'un décideur de niveau hiérarchique suffisamment élevé pour prendre des décisions impliquant l'ensemble de l'organisme
CGI_GDC.3.3	Un responsable et ses remplaçants doivent être identifiés pour chaque cellule de crise
CGI_GDC.3.4	Le responsable d'une cellule de crise doit provoquer une réunion séance tenante de la cellule dès que la procédure de gestion de crise a été déclenchée et qu'il a été informé de la crise
CGI_GDC.3.5	Un nombre suffisant de remplaçants doit être prévu pour chaque membre d'une cellule de crise
CGI_GDC.3.6	Les membres et les remplaçants d'une cellule de crise doivent être sensibilisés et formés à la gestion de crise dans le domaine concerné

4- Attribution des cellules de crise

Code	Libellé
CGI_GDC.4.1	Une cellule de crise doit bénéficier de toutes les informations nécessaires au confinement ou à la résolution d'une crise
CGI_GDC.4.2	Une cellule de crise doit pouvoir prendre toutes les décisions nécessaires au confinement ou à la résolution d'une crise
CGI_GDC.4.3	Les décisions prises par une cellule de crise doivent être mises en œuvre dans les plus brefs délais
CGI_GDC.4.4	Toute décision prise par la cellule de crise doit être consignée par écrit, datée et accompagnée des informations ayant permis la prise de cette décision
CGI_GDC.4.5	La responsabilité de la consignation des décisions d'une cellule de crise doit être attribuée à une personne différente du responsable de la cellule de crise
CGI_GDC.4.6	Les décisions prises par une cellule de crise doivent être conservées, exploitées et gérées comme les autres traces de sécurité du système d'information

3.3.9.2 CGI_LCI : Lutte contre l'incendie

Code	Libellé
CGI_LCI.1.1	Une organisation de lutte contre l'incendie doit être mise en place
CGI_LCI.1.2	L'organisation de lutte contre l'incendie doit être conforme aux normes et standards en vigueur
CGI_LCI.1.3	L'organisation de lutte contre l'incendie doit identifier des profils de lutte contre l'incendie
CGI_LCI.1.4	Le rôle et les responsabilités de chaque profil de lutte contre l'incendie doivent être clairement définis notamment en terme de responsabilité de l'évacuation
CGI_LCI.1.5	Les profils doivent être attribués à des personnes identifiées de l'organisme
CGI_LCI.1.6	Un nombre suffisant de remplaçant doit être prévu pour chaque profil de lutte contre l'incendie
CGI_LCI.1.7	Les titulaires et les remplaçants pour les profils de lutte contre l'incendie doivent être sensibilisés et formés à leurs rôles et leurs responsabilités

3.3.9.3 CGI_GIS : Gestion des incidents de sécurité

1- Incident sur le système d'information

Code	Libellé
CGI_GIS.1.1	Les filières de gestion des incidents doivent être à même de résoudre la plupart des incidents ordinaires dans leur domaine
CGI_GIS.1.2	Les filières de gestion des incidents doivent avoir la possibilité de contacter des niveaux d'escalade supérieurs dans le cas d'incident qu'elles ne pourraient pas traiter
CGI_GIS.1.3	Qu'elles traitent un incident ou pas, les filières de gestion des incidents doivent effectuer un suivi des incidents (type d'incident, date, interlocuteur, suivi des interventions, date de clôture)
CGI_GIS.1.4	Le suivi des incidents non encore résolus doit être régulièrement effectué afin de s'assurer que les recherches de résolution sont en cours
CGI_GIS.1.5	Tout incident résolu doit être archivé avec notamment une description des symptômes de l'incident, de la cause de l'incident et de la méthode de résolution
CGI_GIS.1.6	La procédure de traitement d'incidents de sécurité doit être régulièrement revue afin de s'assurer de son adéquation avec le système d'information et son organisation
CGI_GIS.1.7	Le responsable de la revue de la procédure de traitement d'incidents doit être clairement identifié
CGI_GIS.1.8	Toute modification de la procédure de gestion des incidents doit être diffusée à l'ensemble des utilisateurs du système d'information

2- Vol

Code	Libellé
CGI_GIS.2.1	La filière de gestion des incidents de sécurité liés au vol doit s'occuper des démarches de déclaration de vol auprès des autorités de police
CGI_GIS.2.2	La filière de gestion des incidents de sécurité liés au vol doit imputer le vol sur l'inventaire des biens de l'organisation
CGI_GIS.2.3	La filière de gestion des incidents de sécurité liés au vol doit s'occuper des démarches de résiliation des éventuels éléments d'authentification présents sur le matériel volé
CGI_GIS.2.4	La filière de gestion des incidents de sécurité liés au vol doit s'occuper des éventuelles démarches administratives ou judiciaires nécessaires
CGI_GIS.2.5	Tout incidents de sécurité lié au vol doit être archivé avec notamment la date, l'heure et le lieu ainsi qu'une description des conditions du vol

3- Analyse et reporting

Code	Libellé
CGI_GIS.3.1	Les incidents archivés doivent être analysés pour évaluer s'il est possible d'améliorer la couverture de la vulnérabilité exploitée lors de l'incident et éventuellement pour anticiper des incidents postérieurs (panne ou saturation par exemple)
CGI_GIS.3.2	Les incidents archivés doivent être exploités au sein d'une base de connaissances de manière à accélérer et à simplifier la résolution d'incidents postérieurs du même type
CGI_GIS.3.3	Les incidents archivés doivent être synthétisés et transmis avec les résultats d'analyse à des responsables décisionnels identifiés pour prise en compte dans la stratégie sécurité de l'organisme
CGI_GIS.3.4	Les responsables décisionnels assurant l'analyse de la synthèse des incidents et leurs remplaçants doivent être clairement identifiés
CGI_GIS.3.5	Les responsables décisionnels assurant l'analyse de la synthèse des incidents et leurs remplaçants doivent être sensibilisés et formés à ce type d'analyse
CGI_GIS.3.6	Les responsables décisionnels assurant l'analyse de la synthèse des incidents ou le cas échéant leurs remplaçants doivent avoir la possibilité de prendre des décisions permettant de pallier les évolutions prévisibles

3.3.10 CEI : Études initiales et conception du SI

3.3.10.1 CEI_ABS : Analyse des besoins de sécurité

Code	Libellé
CEI_ABS.1.1	La sécurisation des parties non mutualisées du système d'information doit être effectuée en fonction des besoins de sécurité des composants fonctionnels concernés
CEI_ABS.1.2	Chaque composant fonctionnel doit faire l'objet d'une étude visant à déterminer ses besoins de sécurité, notamment en terme de confidentialité, de disponibilité, d'intégrité et de contrôle/preuve
CEI_ABS.1.3	Tout besoin spécifique non couvert par les dispositions de sécurité générales du système d'information doit si possible être couvert par des dispositions spécifiques à l'élément fonctionnel (architecture technique, procédures sécurité…)
CEI_ABS.1.4	Tout besoin spécifique qui ne peut pas être couvert de façon satisfaisante doit faire l'objet d'une étude de risques résiduels (voir CRR_ETU)
CEI_ABS.1.5	L'étude initiale doit permettre d'évaluer les ressources nécessaires et d'obtenir un premier dimensionnement du système (en période de pointe et secours inclus) et des équipes (remplaçants inclus) ainsi que des ressources nécessaires à son développement
CEI_ABS.1.6	Les besoins de sécurité identifiés doivent tenir compte des enjeux et du contexte environnant local (économique, social, politique, législatif…)
CEI_ABS.1.7	Les besoins de sécurité identifiés doivent tenir compte des impacts potentiels d'un incident

3.3.10.2 CEI_CDT : Choix des technologies

1- Pérennité

Code	Libellé
CEI_CDT.1.1	La pérennité doit être un facteur de choix majeur lors de la sélection des technologies pour le système d'information (matériels, applications, langages de développement…)
CEI_CDT.1.2	Les technologies désuètes du système d'information doivent être remplacées le plus rapidement possible par des technologies pérennes

2- Ergonomie

Code	Libellé
CEI_CDT.2.1	L'ergonomie d'utilisation et d'exploitation doit être prise en compte lors du choix des logiciels, matériels et installations
CEI_CDT.2.2	Les normes et standards sanitaires doivent être prise en compte lors du choix des logiciels, matériels et installations

3.3.10.3 CEI_ERS : Étude des risques spécifiques liés aux matériels et logiciels utilisés

Code	Libellé
CEI_ERS.1.1	Les éventuels risques spécifiques aux éléments hébergés dans l'organisme (matériel explosif, produits inflammables, sources de rayonnement électromagnétique ou thermique...) doivent être étudiés et pris en compte lors de l'installation des sites

3.3.11 CPS : Politiques de sécurité

3.3.11.1 CPS_PPT : Politique de protection des postes de travail

Code	Libellé
CPS_PPT.1.1	La politique de sécurité doit inclure une politique de protection des postes de travail fixes et nomades (intégrité, contrôle d'accès, lutte contre les codes malveillants…)

Code	Libellé
CPS_PPT.1.2	La politique de protection des postes de travail doit être adaptée aux besoins de sécurité de l'organisme
CPS_PPT.1.3	La politique de protection des postes de travail doit être revue régulièrement pour valider son adéquation avec les besoins de sécurité de l'organisme
CPS_PPT.1.4	Le responsable de la revue de la politique de protection des postes de travail doit être clairement identifié
CPS_PPT.1.5	Toute modification de la politique de protection des postes de travail doit faire l'objet d'une communication à l'ensemble des utilisateurs de poste de travail

3.3.11.2 CPS_PAQ : Politique d'Assurance Qualité

1- Manuel d'Assurance Qualité

Code	Libellé
CPS_PAQ.1.1	Les opérations réalisées sur le système d'information doivent être couvertes par le Plan d'Assurance Qualité de l'organisme
CPS_PAQ.1.2	Les dispositions du Plan d'Assurance Qualité de l'organisme doivent être consignées dans un Manuel d'Assurance Qualité
CPS_PAQ.1.3	Tous les employés de l'organisme doivent avoir accès au Manuel d'Assurance Qualité
CPS_PAQ.1.4	Le Manuel d'Assurance Qualité doit être revu régulièrement pour s'assurer de son adéquation avec les objectifs qualité de l'organisme
CPS_PAQ.1.5	Le responsable de la revue du Manuel d'Assurance Qualité doit être clairement identifié
CPS_PAQ.1.6	Toute modification du Manuel d'Assurance Qualité doit faire l'objet d'une communication à l'ensemble des employés de l'organisme

2- Adhésion du personnel à la démarche Qualité

Code	Libellé
CPS_PAQ.2.1	Le Manuel d'Assurance Qualité doit traiter les aspects d'assurance qualité métier
CPS_PAQ.2.2	L'ensemble des employés de l'organisme doivent être sensibilisés aux dispositions qualité métier de manière à adhérer à la démarche qualité

3- Disposition Qualité

Code	Libellé
CPS_PAQ.3.1	Dans la mesure du possible, les traitements manuels doivent être validés par un responsable avant d'être utilisés

3.3.11.3 CPS_DEV : Politique de sécurité pour le développement

Code	Libellé
CPS_DEV.1.1	Le développement d'applications pour le système d'information doit être maîtrisé et encadré par des règles de développement
CPS_DEV.1.2	Les règles de développement doivent s'appuyer sur des normes et standards de développement nationaux et internationaux

3.3.12 CPD : Protection des données

3.3.12.1 CPD_DGL : Données de géolocalisation

Code	Libellé
CPD_DGL.1.1	Les données exploitables pour localiser une personne ou un matériel doivent être considérées comme des données sensibles et protégées comme telles en confidentialité
CPD_DGL.1.2	Le personnel de l'organisation doit être sensibilisé à la protection des données exploitables pour localiser une personne ou un matériel

3.3.12.2 CPD_INP : Identification des niveaux de protection

Code	Libellé
CPD_INP.1.1	Le niveau de protection d'un système doit être identifié physiquement sur le système ainsi que dans la documentation qui lui est consacrée

3.3.13 CFO : Formation

3.3.13.1 CFO_SPS : Sensibilisation sur les problèmes de sécurité

Code	Libellé
CFO_SPS.1.1	L'ensemble des utilisateurs du système d'information doit être sensibilisé aux risques pesant sur le système d'information, aux méthodes d'attaque, aux problèmes de sécurité potentiels et aux mesures pour couvrir les risques ou en limiter les impacts
CFO_SPS.1.2	L'ensemble du personnel doit être sensibilisé aux comportements anodins susceptibles de dégradés la qualité de service du système d'information (forward d'hoax par exemple)

3.3.13.2 CFO_FRS : Formation des remplaçants ou successeurs

1- Remplaçants

Code	Libellé
CFO_FRS.1.1	Un nombre adapté de remplaçants doit être identifié pour les fonctions importantes de l'organisation au cas où leurs titulaires seraient ponctuellement indisponibles
CFO_FRS.1.2	Les remplaçants identifiés pour prendre en charge des fonctions ponctuellement vacantes doivent être formés aux tâches associées à ces fonctions
CFO_FRS.1.3	Les remplaçants identifiés pour prendre en charge des fonctions ponctuellement vacantes doivent être informés des responsabilités associées à ces fonctions
CFO_FRS.1.4	Selon les fonctions nécessitant remplacement, un remplaçant peut être déchargé d'une partie ou de toutes ses fonctions habituelles
CFO_FRS.1.5	Lors d'un remplacement, le remplaçant doit bénéficier de tous les privilèges, droits, attributions et responsabilité de la personne remplacée

2- Successeurs

Code	Libellé
CFO_FRS.2.1	Dans la mesure du possible, le départ du titulaire d'une fonction doit être prévu et préparé le plus tôt possible
CFO_FRS.2.2	Si, après le départ d'un titulaire, le dimensionnement d'une équipe n'est plus adaptée aux fonctions dont elle a la charge, un successeur doit être identifié pour le titulaire partant
CFO_FRS.2.3	Une période de transition suffisamment longue doit être prévue pendant laquelle le titulaire partant et son successeur occupe les mêmes fonctions
CFO_FRS.2.4	Avant son départ, un titulaire partant doit former son successeur et le présenter à ses interlocuteurs habituels

3.3.14 CCC : Clauses contractuelles

3.3.14.1 CCC_CLR : Clauses contractuelles limitant les responsabilités des 2 parties

Code	Libellé
CCC_CLR.1.1	Les responsabilités, sanctions et pénalité attribuées à chaque partie signataire d'un contrat doivent être adaptées au contexte et en rapport avec les impacts potentiels (les pénalités et les sanctions démesurées sont à éviter)
CCC_CLR.1.2	Les responsabilités de chaque partie signataire d'un contrat doivent être limitées par un maximum clairement identifié

3.3.14.2 CCC_RGF : Réversibilité et garanties financières

Code	Libellé

Code	Libellé
CCC_RGF.1.1	Des mesures d'évaluation de la pérennité financière et/ou technique doivent être mises en place lors de la sélection d'un sous-traitant ou d'un prestataire
CCC_RGF.1.2	Les contrats de sous-traitance et les contrats de prestation de longue durée doivent intégrer une clause de réversibilité

3.3.15 CRH : Ressources humaines

3.3.15.1 CRH_DDE : Dimensionnement des équipes

Code	Libellé
CRH_DDE.1.1	Les équipes doivent être dimensionnées pour pouvoir assurer de façon satisfaisante leurs fonctions
CRH_DDE.1.2	Les équipes doivent être dimensionnées pour pouvoir assurer leurs fonctions essentielles en cas d'indisponibilité d'une partie de leurs membres

3.3.15.2 CRH_PDP : Protection du personnel

Code	Libellé
CRH_PDP.1.1	En cas d'environnement général difficile, l'organisation doit mettre en place des mesures de protection du personnel (service de protection, hébergement proche du site…)
CRH_PDP.1.2	Les personnels travaillant dans des sites distants doivent pouvoir être hébergés de façon temporaire dans le site principal et avoir la possibilité d'y mener ses missions les plus importantes
CRH_PDP.1.3	L'organisme doit prévoir la mise en place de solutions de secours en cas de difficulté d'accès au site (car de ramassage en cas de grèves des transports, location de chasse neige pour dégager l'accès au site…)

3.3.15.3 CRH_CDT : Conditions de travail

Code	Libellé
CRH_CDT.1.1	L'aménagement des locaux doit être le plus favorable possible au travail demandé (éclairage suffisant, température adaptée, isolation phonique, espace de rangement…)
CRH_CDT.1.2	Des dispositions spécifiques doivent être prises afin de réduire les perturbations sur le lieu de travail (pas de réunion dans des open-space, machine à café à l'écart des espaces de travail…)

3.3.15.4 CRH_QDP : Qualification du personnel

Code	Libellé
CRH_QDP.1.1	Les missions attribuées à chaque employé doivent correspondre à ses qualifications

3.3.16 CDS : Dimensionnement des systèmes

3.3.16.1 CDS_DES : Dimensionnement des services essentiels

Code	Libellé
CDS_DES.1.1	Les services essentiels et les secours doivent être dimensionnés de manière à offrir des services adaptés et de qualité y compris lors des éventuelles périodes de pointe
CDS_DES.1.2	Le dimensionnement des services essentiels doit être revu régulièrement et à chaque évolution majeure du système d'information ou des sites afin les services restent adaptés et de qualité y compris lors des éventuelles périodes de pointe

4 Détermination des objectifs et exigences de sécurité

Les objectifs et exigences de sécurité fonctionnelles (dont les codes correspondent à ceux des parties précédentes) sont présentés par menace générique, c'est-à-dire par type d'entités, méthode d'attaque (MA) et vulnérabilité. Les menaces correspondant aux sous-types d'entités héritent des objectifs et exigences de sécurité fonctionnelles du type d'entités.
D'une part, les tableaux suivants permettent de déterminer aisément les objectifs de sécurité génériques susceptibles de couvrir chaque vulnérabilité générique. Ils sont donc utile au traitement des vulnérabilités, mais devront être complétés par des objectifs couvrant les origines et conséquences des risques pour traiter pleinement ces risques.
D'autre part, ils permettent de déterminer aisément les exigences de sécurité fonctionnelles génériques susceptibles de satisfaire chaque objectif de sécurité générique.

4.1 MAT : Matériel

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT	6	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels	PHY_01	BPE_SEM.4.1
MAT	6	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels	PHY_01	BPE_SEM.2.1
MAT	6	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels	PHY_01	CAR_AAR.1.1
MAT	9	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels	PHY_01	BPE_SEM.4.1
MAT	9	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels	PHY_01	CAR_AAR.1.1
MAT	9	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels	PHY_01	BPE_SEM.2.1
MAT	17	Matériel susceptible d'émettre des rayonnements parasites compromettants	PHY_05	BPE_SEM.3.1
MAT	17	Absence de prise en compte des règles d'installation	MAT_14	CGS_OML.1.1
MAT	17	Absence de prise en compte du zonage des matériels	PHY_03	CIS_PSI.1.2
MAT	17	Absence de prise en compte du zonage des matériels	PHY_03	CIS_PSI.1.1
MAT	28	Mauvaises conditions d'utilisation	MAT_14	CGS_OML.1.1
MAT	28	Absence de protection contre les perturbations électriques	PHY_03	CIS_PSI.1.1
MAT	28	Absence de protection contre les perturbations électriques	PHY_03	CIS_PSI.1.2
MAT	29	Mauvaises conditions d'utilisation	MAT_14	CGS_OML.1.1
MAT	29	Absence de protection contre les perturbations électriques	PHY_03	CIS_PSI.1.1
MAT	29	Absence de protection contre les perturbations électriques	PHY_03	CIS_PSI.1.2
MAT	30	Mauvais dimensionnement des ressources (ex: manque d'autonomie d'une batterie de portable)	MAT_09	BGC_PRS.1.1
MAT	30	Mauvais dimensionnement des ressources (ex: manque d'autonomie d'une batterie de portable)	MAT_09	CEI_ABS.1.5
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.2
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT	38	Matériel d'utilisation complexe ou peu ergonomique	MAT_11	BSP_FOU.2.1
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.2
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.1
MAT	38	Mauvaises conditions d'utilisation	MAT_14	CGS_OML.1.1
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.2
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.1
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.3
MAT	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.3

4.1.1 MAT_ACT : Support de traitement de données (actif)

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT	1	Absence de matériels de remplacement	MAT_01	FRU_FLT.2.1
MAT_ACT	1	Absence de matériels de remplacement	MAT_01	FRU_FLT.1.1
MAT_ACT	1	Matériel utilisant des matériaux inflammables (ex. : imprimantes de masse provoquant des poussières)	PHY_09	CIS_CSI.1.1
MAT_ACT	1	Matériel utilisant des matériaux inflammables (ex. : imprimantes de masse provoquant des poussières)	PHY_09	CIS_CSI.1.2
MAT_ACT	2	Absence de matériels de remplacement	MAT_01	FRU_FLT.2.1
MAT_ACT	2	Absence de matériels de remplacement	MAT_01	FRU_FLT.1.1
MAT_ACT	4	Absence de matériels de remplacement	MAT_01	FRU_FLT.2.1
MAT_ACT	4	Absence de matériels de remplacement	MAT_01	FRU_FLT.1.1
MAT_ACT	5	Absence de matériels de remplacement	MAT_01	FRU_FLT.2.1
MAT_ACT	5	Fragilité des matériels	ORG_04	BPE_SEM.1.1
MAT_ACT	5	Fragilité des matériels	ORG_04	BSP_FOU.1.1
MAT_ACT	5	Fragilité des matériels	ORG_04	BPE_SEM.2.1
MAT_ACT	5	Matériel accessible à des personnes autres que leurs propriétaires (ex: placé dans un lieu de passage)	PHY_03	CIS_PSI.1.1
MAT_ACT	5	Matériel accessible à des personnes autres que leurs propriétaires (ex: placé dans un lieu de passage)	PHY_03	CIS_PSI.1.2
MAT_ACT	5	Absence de matériels de remplacement	MAT_01	FRU_FLT.1.1
MAT_ACT	7	Matériel sensible aux vibrations	PHY_03	CIS_PSI.1.1
MAT_ACT	7	Matériel sensible aux vibrations	PHY_03	CIS_PSI.1.2
MAT_ACT	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)	PHY_01	CAR_AAR.1.1
MAT_ACT	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)	PHY_01	BPE_SEM.4.1
MAT_ACT	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)	PHY_01	BPE_SEM.2.1
MAT_ACT	13	Matériel maintenu à distance par des moyens de télécommunication	PHY_01	CAR_AAR.1.1
MAT_ACT	13	Matériel maintenu à distance par des moyens de télécommunication	PHY_01	BPE_SEM.4.1
MAT_ACT	13	Matériel maintenu à distance par des moyens de télécommunication	PHY_01	BPE_SEM.2.1
MAT_ACT	19	Accès logique au matériel permettant la pose d'un logiciel d'écoute	MAT_10	CGS_GLI.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT	19	Matériel disposant d'interface de communication écoutable (infra rouge, 802.11, Bluetooth…)	RES_02	BMA_MAR.1.1
MAT_ACT	19	Matériel disposant d'interface de communication écoutable (infra rouge, 802.11, Bluetooth…)	RES_02	CGS_PPS.1.3
MAT_ACT	19	Matériel disposant d'interface de communication écoutable (infra rouge, 802.11, Bluetooth…)	RES_02	CGS_PPS.1.2
MAT_ACT	19	Accès logique au matériel permettant la pose d'un logiciel d'écoute	MAT_10	BPE_SEM.1.1
MAT_ACT	19	Matériel disposant d'interface de communication écoutable (infra rouge, 802.11, Bluetooth…)	RES_02	BMA_GAU.2.1
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.5.1
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.1
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.1.1
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.10
MAT_ACT	20	Absence d'inventaire du matériel	MAT_06	BCM_RLC.1.1
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.2
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.2.3
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.9
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.8
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BCM_RLC.1.1
MAT_ACT	21	Absence de matériels de remplacement	MAT_01	FRU_FLT.2.1
MAT_ACT	21	Absence de matériels de remplacement	MAT_01	FRU_FLT.1.1
MAT_ACT	24	Absence de moyens permettant de garantir la provenance d'un matériel	ORG_20	CGS_OML.1.1
MAT_ACT	25	Possibilité de pose d'éléments matériels additionnels pour stocker, transmettre ou altérer (ex: keylogger physique)	MAT_10	BPE_SEM.1.1
MAT_ACT	28	Vieillissement du matériel	ORG_13	BPE_SEM.4.1
MAT_ACT	28	Mauvaise fiabilité des matériels	MAT_15	BGC_PRS.2.1
MAT_ACT	28	Défaut de maintenance	ORG_27	CET_EIP.1.3
MAT_ACT	28	Défaut de maintenance	ORG_27	CGS_GMA.2.1
MAT_ACT	28	Défaut de maintenance	ORG_27	CGS_GMA.1.2
MAT_ACT	29	Mauvaise fiabilité des matériels	MAT_15	BGC_PRS.2.1
MAT_ACT	29	Possibilité d'incompatibilité entre les différents matériels	RES_04	BGC_PRS.2.1
MAT_ACT	32	Matériels obsolètes	ORG_13	BPE_SEM.4.1
MAT_ACT	32	Absence de moyens de support accessible depuis l'extérieur de l'organisme ou depuis un pays dont le décalage horaire est important	MAT_13	CGS_GSU.1.3
MAT_ACT	32	Absence de moyens de support accessible depuis l'extérieur de l'organisme ou depuis un pays dont le décalage horaire est important	MAT_13	CGS_GSU.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT	32	Matériels spécifiques	ORG_27	BGC_PRS.2.1
MAT_ACT	32	Matériels à configurations non évolutives	ORG_13	BPE_SEM.4.1
MAT_ACT	33	Le matériel utilisé permet un autre usage que celui qui est prévu (développement de logiciels non destinés à l'organisme…)	LOG_11	CGS_GDH.2.1
MAT_ACT	33	Le matériel est connecté à des réseaux externes	MAT_10	FTA_TAB.1.1
MAT_ACT	33	Le matériel utilisé permet un autre usage que celui qui est prévu (développement de logiciels non destinés à l'organisme…)	LOG_11	CGS_GDH.1.2
MAT_ACT	33	Le matériel utilisé permet un autre usage que celui qui est prévu (développement de logiciels non destinés à l'organisme…)	PER_03	CGS_GDH.1.2
MAT_ACT	33	Le matériel utilisé permet un autre usage que celui qui est prévu (développement de logiciels non destinés à l'organisme…)	PER_03	CGS_GDH.2.1
MAT_ACT	38	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes…)	MAT_11	CEI_CDT.2.1
MAT_ACT	38	Absence de responsabilité	PER_05	BSP_SPR.4.1
MAT_ACT	38	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes…)	MAT_11	CEI_CDT.2.2
MAT_ACT	38	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes…)	MAT_11	BSP_FOU.2.1
MAT_ACT	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.2.1
MAT_ACT	38	Absence de responsabilité	PER_05	BSP_SPR.1.1
MAT_ACT	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.1.1
MAT_ACT	39	Absence de protection physique	PHY_03	CIS_PSI.1.1
MAT_ACT	39	Absence de protection physique	PHY_03	CIS_PSI.1.2
MAT_ACT	40	Le matériel est connecté à des réseaux externes	MAT_10	BPE_SEM.1.1
MAT_ACT	41	Absence de dispositif de traces et d'audit	ORG_39	BDM_COC.4.1
MAT_ACT	41	Le matériel est accessible et utilisable par tous	MAT_10	BPE_SEM.1.1
MAT_ACT	42	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes…)	MAT_12	BSP_FOU.2.1
MAT_ACT	42	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes…)	MAT_12	CEI_CDT.2.1
MAT_ACT	42	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes…)	MAT_12	CEI_CDT.2.2

4.1.1.1 MAT_ACT.1 : Matériel transportable

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.1	18	Écran observable depuis l'extérieur	PHY_02	CIS_ADL.1.1
MAT_ACT.1	18	Écran observable depuis l'extérieur	PHY_02	BPE_MMG.1.1
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.1.8

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.1.10
MAT_ACT.1	20	Disque dur facilement démontable	MAT_07	CET_EGT.2.3
MAT_ACT.1	20	Absence de protection des matériels contre le vol (câble anti-vol)	MAT_07	CET_EGT.2.3
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.2.3
MAT_ACT.1	20	Disque dur facilement démontable	MAT_07	CET_EGT.1.10
MAT_ACT.1	20	Absence de protection des matériels contre le vol (câble anti-vol)	MAT_07	BCM_RLC.1.1
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	BCM_RLC.1.1
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	BMA_REU.2.1
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	BPE_SEM.1.1
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CGS_PPS.3.1
MAT_ACT.1	20	Disque dur facilement démontable	MAT_07	CET_EGT.1.8
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.1.9
MAT_ACT.1	20	Absence de protection des matériels contre le vol (câble anti-vol)	MAT_07	CGS_PPS.3.1
MAT_ACT.1	20	Absence de protection des matériels contre le vol (câble anti-vol)	MAT_07	BPE_SEM.5.1
MAT_ACT.1	20	Disque dur facilement démontable	MAT_07	CGS_PPS.3.2
MAT_ACT.1	20	Disque dur facilement démontable	MAT_07	CET_EGT.1.9
MAT_ACT.1	20	Disque dur facilement démontable	MAT_07	BPE_SEM.1.1
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.8
MAT_ACT.1	21	Revente possible du matériel (absence de marquage, utilisation sans mot de passe)	MAT_07	FIA_UID.1.2/2.1
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.10
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.1.1
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	BPE_SEM.1.1
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.2.3
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	BMA_REU.2.1
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BCM_RLC.1.1
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	BCM_RLC.1.1
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.1
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.9
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.5.1
MAT_ACT.1	21	Revente possible du matériel (absence de marquage, utilisation sans mot de passe)	MAT_07	CGS_PPS.2.1
MAT_ACT.1	21	Revente possible du matériel (absence de marquage, utilisation sans mot de passe)	MAT_07	FIA_UAU.6.1
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.1.10
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.2.3
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.1.9
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CGS_PPS.3.1
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes	MAT_07	CET_EGT.1.8
MAT_ACT.1	21	Absence d'inventaire du matériel	MAT_06	BCM_RLC.1.1
MAT_ACT.1	21	Revente possible du matériel (absence de marquage, utilisation sans mot de passe)	MAT_07	FIA_UAU.1.2/2.1
MAT_ACT.1	22	Présence de données résiduelles à l'insu de l'utilisateur de matériels ré-attribués ou mis au rebut	MAT_08	BGC_MSS.2.1
MAT_ACT.1	26	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)	MAT_10	BPE_SEM.1.1
MAT_ACT.1	27	Matériel localisable (ex: triangularisation)	PHY_05	CPD_DGL.1.1
MAT_ACT.1	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité…)	LOG_11	CGS_GDH.1.2
MAT_ACT.1	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité…)	LOG_11	CGS_GDH.2.1
MAT_ACT.1	34	Matériel permettant l'enregistrement de données sur support (disquette, ZIP, graveur cédérom/DVD)	ORG_15	BDM_COC.2.1
MAT_ACT.1	36	Matériels obsolètes	ORG_13	BPE_SEM.4.1
MAT_ACT.1	36	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)	MAT_10	BPE_SEM.1.1
MAT_ACT.1	36	Absence de règles de protection des données	ORG_15	BDM_COC.2.1
MAT_ACT.1	39	Absence de dispositif de contrôle d'accès robuste	MAT_10	BPE_SEM.1.1
MAT_ACT.1	40	Absence de dispositif de contrôle d'accès robuste	MAT_10	BPE_SEM.1.1

4.1.1.2 MAT_ACT.2 : Matériel fixe

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.2	11	Matériel nécessitant une climatisation pour fonctionner	MAT_03	BMA_MAA.2.1
MAT_ACT.2	11	Matériel nécessitant une climatisation pour fonctionner	PHY_01	BPE_SEM.2.1
MAT_ACT.2	11	Matériel nécessitant une climatisation pour fonctionner	PHY_01	CAR_AAR.1.1
MAT_ACT.2	11	Matériel nécessitant une climatisation pour fonctionner	PHY_01	BPE_SEM.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.2	11	Matériel nécessitant une climatisation pour fonctionner	MAT_03	BPE_SEM.1.1
MAT_ACT.2	14	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques	PHY_03	CIS_PSI.1.1
MAT_ACT.2	14	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques	PHY_03	CIS_PSI.1.2
MAT_ACT.2	15	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques	PHY_03	CIS_PSI.1.1
MAT_ACT.2	15	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques	PHY_03	CIS_PSI.1.2
MAT_ACT.2	16	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques	PHY_03	CIS_PSI.1.1
MAT_ACT.2	16	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques	PHY_03	CIS_PSI.1.2
MAT_ACT.2	18	Ecran observable depuis l'extérieur	PHY_02	BPE_MMG.1.1
MAT_ACT.2	18	Ecran observable depuis l'extérieur	PHY_02	CIS_ADL.1.1
MAT_ACT.2	20	Disque dur facilement démontable	MAT_07	CET_EGT.1.10
MAT_ACT.2	20	Disque dur facilement démontable	MAT_07	CET_EGT.1.8
MAT_ACT.2	20	Disque dur facilement démontable	MAT_07	CET_EGT.1.9
MAT_ACT.2	20	Disque dur facilement démontable	MAT_07	CGS_PPS.3.2
MAT_ACT.2	20	Disque dur facilement démontable	MAT_07	BPE_SEM.1.1
MAT_ACT.2	20	Disque dur facilement démontable	MAT_07	CET_EGT.2.3
MAT_ACT.2	21	Matériel facilement démontable	MAT_07	CET_EGT.1.10
MAT_ACT.2	21	Matériel facilement démontable	MAT_07	CET_EGT.1.8
MAT_ACT.2	21	Matériel facilement démontable	MAT_07	BPE_SEM.1.1
MAT_ACT.2	21	Matériel facilement démontable	MAT_07	CGS_PPS.3.2
MAT_ACT.2	21	Matériel facilement démontable	MAT_07	CET_EGT.2.3
MAT_ACT.2	21	Matériel facilement démontable	MAT_07	CET_EGT.1.9
MAT_ACT.2	22	Présence de données résiduelles à l'insu de l'utilisateur de matériels ré-attribués ou mis au rebut	MAT_08	BGC_MSS.2.1
MAT_ACT.2	23	Fonctions de gestion des droits d'accès trop compliquées à utiliser et pouvant être source d'erreur	MAT_11	BSP_FOU.2.1
MAT_ACT.2	23	Présence de répertoire partagé pour stocker de l'information	MAT_10	BGC_MSS.3.1
MAT_ACT.2	23	Procédures de gestion des privilèges d'accès trop lourde à opérer	ORG_36	CGS_PAI.1.4
MAT_ACT.2	23	Absence de vérification des accès partagés accordés	MAT_10	BGC_MSS.3.1
MAT_ACT.2	26	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)	MAT_10	BPE_SEM.1.1
MAT_ACT.2	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité…)	LOG_11	CGS_GDH.1.2
MAT_ACT.2	34	Matériel permettant l'enregistrement de données sur support (disquette, ZIP, graveur cédérom/DVD)	ORG_15	BDM_COC.2.1
MAT_ACT.2	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité…)	LOG_11	CGS_GDH.2.1
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_SVG.1.4

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_SVG.1.8
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_GSS.1.1
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_GSS.1.1
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_SVG.1.7
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_SVG.1.3
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_SVG.1.3
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_SVG.1.9
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	BGC_PRE.1.1
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_SVG.1.9
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_SVG.1.5
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	BGC_INT.1.1
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_SVG.1.5
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_SVG.1.6
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_SVG.1.4
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	BGC_PRE.1.1
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_SVG.1.7
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	CGS_SVG.1.8
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	MAT_01	CGS_SVG.1.6
MAT_ACT.2	36	Matériels obsolètes	ORG_13	BPE_SEM.4.1
MAT_ACT.2	36	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)	MAT_10	BPE_SEM.1.1
MAT_ACT.2	36	Absence de règles de protection des données	ORG_15	BDM_COC.2.1
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde	ORG_08	BGC_INT.1.1
MAT_ACT.2	39	Absence de dispositif de contrôle d'accès robuste	MAT_10	BPE_SEM.1.1
MAT_ACT.2	40	Absence de dispositif de contrôle d'accès robuste	MAT_10	BPE_SEM.1.1

4.1.1.3 MAT_ACT.3 : Périphérique de traitement

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.3	11	Matériel nécessitant une climatisation pour fonctionner	PHY_01	BPE_SEM.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.3	11	Matériel nécessitant une climatisation pour fonctionner	PHY_01	CAR_AAR.1.1
MAT_ACT.3	11	Matériel nécessitant une climatisation pour fonctionner	PHY_01	BPE_SEM.4.1
MAT_ACT.3	11	Matériel nécessitant une climatisation pour fonctionner	MAT_03	BPE_SEM.1.1
MAT_ACT.3	11	Matériel nécessitant une climatisation pour fonctionner	MAT_03	BMA_MAA.2.1
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage	PER_02	CET_EGT.2.3
MAT_ACT.3	20	Absence de protection d'accès aux équipements de sauvegarde	MAT_07	CET_EGT.2.3
MAT_ACT.3	20	Absence de protection d'accès aux équipements de sauvegarde	MAT_07	BPE_SEM.1.1
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage	ORG_01	CET_EGT.3.1
MAT_ACT.3	20	Absence de protection d'accès aux équipements de sauvegarde	MAT_07	CET_EGT.3.1
MAT_ACT.3	20	Absence de protection d'accès aux équipements de sauvegarde	MAT_07	BPE_ZOS.1.1
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage	PER_02	BPS_PSI.1.5
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage	PER_02	BSP_FOU.1.1
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage	ORG_01	BPE_ZOS.1.1
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage	ORG_01	BPE_ZOS.2.1
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage	ORG_01	BPE_SEM.1.1
MAT_ACT.3	20	Absence de protection d'accès aux équipements de sauvegarde	MAT_07	BPE_ZOS.2.1
MAT_ACT.3	21	Absence d'inventaire du matériel	MAT_06	BCM_RLC.1.1
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.1.1
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BCM_RLC.1.1
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.5.1
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.2
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.1
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.9
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.8
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.10
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.2.3
MAT_ACT.3	36	Usure des supports	MAT_14	CGS_OML.1.1
MAT_ACT.3	36	Absence de moyens de protection et de contrôle de l'intégrité des données	LOG_01	FDP_ITT.3.1
MAT_ACT.3	36	Absence de moyens de protection et de contrôle de l'intégrité des données	LOG_01	FDP_ITT.3/4.2
MAT_ACT.3	37	Absence de protection physique	PHY_03	CIS_PSI.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_ACT.3	37	Absence de protection physique	PHY_03	CIS_PSI.1.1
MAT_ACT.3	40	Absence de cloisonnement des équipements	MAT_10	BPE_ZOS.2.1
MAT_ACT.3	40	Absence de cloisonnement des équipements	MAT_10	BPE_SEM.1.1
MAT_ACT.3	40	Absence de cloisonnement des équipements	MAT_10	BGC_PRE.4.1

4.1.2 MAT_PAS : Support de données (passif)

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS	3	Support sensible aux conditions de conservation	MAT_03	BPE_SEM.1.1
MAT_PAS	3	Support sensible aux conditions de conservation	MAT_03	BMA_MAA.2.1
MAT_PAS	5	Fragilité des supports	ORG_04	BSP_FOU.1.1
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.9
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.5
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.3
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.6
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.7
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.4
MAT_PAS	5	Absence de mesures de conservation des archives adaptées aux délais de rétention (vieillissement des bandes, usure du cédérom)	MAT_04	CGS_ARC.1.1
MAT_PAS	5	Absence de mesures de conservation des archives adaptées aux délais de rétention (vieillissement des bandes, usure du cédérom)	MAT_04	CGS_ARC.1.2
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.8
MAT_PAS	5	Absence de procédure d'archivage	ORG_07	BGC_PRE.1.1
MAT_PAS	5	Support accessible à des personnes autres que leurs propriétaires	PHY_03	CIS_PSI.1.1
MAT_PAS	5	Support accessible à des personnes autres que leurs propriétaires	PHY_03	CIS_PSI.1.2
MAT_PAS	5	Fragilité des supports	ORG_04	BPE_SEM.2.1
MAT_PAS	5	Fragilité des supports	ORG_04	BPE_SEM.1.1
MAT_PAS	20	Les supports sont accessibles par tous	MAT_07	CET_EGT.2.3
MAT_PAS	20	Absence de protection du stockage des supports	MAT_07	CET_EGT.2.3
MAT_PAS	20	Les supports sont accessibles par tous	MAT_07	BPE_ZOS.1.1
MAT_PAS	20	Transmission des supports par des services postaux (fournisseurs externes, courrier interne…)	ORG_03	BGC_EIL.2.1
MAT_PAS	20	Les supports sont accessibles par tous	MAT_07	CGS_PPS.3.2
MAT_PAS	20	Absence de protection du stockage des supports	MAT_07	CGS_PPS.3.2
MAT_PAS	20	Les supports sont accessibles par tous	MAT_07	BPE_ZOS.2.1
MAT_PAS	22	Absence de moyens de destruction des supports	MAT_08	BGC_MSS.2.1
MAT_PAS	23	Supports capables d'effectuer des échanges d'information à caractère sensible	MAT_10	BGC_EIL.2.1
MAT_PAS	33	Les supports sont accessibles par tous	ORG_30	BPE_ZOS.1.1
MAT_PAS	33	Les supports sont accessibles par tous	ORG_30	BPE_ZOS.2.1
MAT_PAS	33	Les supports sont accessibles par tous	ORG_30	CGS_PPS.3.2
MAT_PAS	36	Absence de moyens de protection et de contrôle de l'intégrité des données	LOG_01	BDM_COC.3.1
MAT_PAS	36	Usure des supports	MAT_14	CGS_OML.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS	37	Les supports sont accessibles par tous	ORG_30	CET_EGT.2.3
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	CET_EGT.1.10
MAT_PAS	37	Les supports sont accessibles par tous	ORG_30	CGS_PPS.3.2
MAT_PAS	37	Les supports sont accessibles par tous	ORG_30	BPE_ZOS.1.1
MAT_PAS	37	Absence de moyen d'identification de la sensibilité des informations contenues sur les supports	ORG_15	BDM_COC.2.1
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.8
MAT_PAS	37	Les supports sont accessibles par tous	ORG_30	BPE_ZOS.2.1
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.2.3
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.10
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.1
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BSP_RIS.5.2
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.1.1
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_ZOS.2.1
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_ZOS.1.1
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BCM_RLC.1.1
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	CET_EGT.2.3
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	BPE_SEM.5.1
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	CGS_PPS.3.2
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	BCM_RLC.1.1
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	BPE_SEM.1.1
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	BPE_SEM.5.1
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CET_EGT.1.9
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	BPE_ZOS.1.1
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	BPE_ZOS.2.1
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	CET_EGT.1.9
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur extractible)	MAT_07	CET_EGT.1.8
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)	MAT_07	CGS_PPS.3.2
MAT_PAS	38	Absence de labellisation des supports	MAT_06	BCM_RLC.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS	41	Les supports sont accessibles par tous	ORG_15	BDM_COC.2.1
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.9
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.6
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.8
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.5
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.4
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.3
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	CGS_ARC.1.7
MAT_PAS	42	Absence de procédure d'archivage	ORG_07	BGC_PRE.1.1

4.1.2.1 MAT_PAS.1 : Support électronique

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS.1	1	Absence de sauvegarde des données contenues sur les supports	ORG_08	BGC_INT.1.1
MAT_PAS.1	1	Absence de sauvegarde des données contenues sur les supports	ORG_08	CGS_GLI.1.2
MAT_PAS.1	1	Absence de sauvegarde des données contenues sur les supports	ORG_08	CGS_SVG.1.1
MAT_PAS.1	1	Absence de sauvegarde des données contenues sur les supports	ORG_08	CGS_SVG.1.2
MAT_PAS.1	2	Absence de sauvegarde des données contenues sur les supports	ORG_08	BGC_INT.1.1
MAT_PAS.1	4	Absence de sauvegarde des données contenues sur les supports	ORG_08	BGC_INT.1.1
MAT_PAS.1	5	Absence de sauvegarde des données contenues sur les supports	ORG_08	BGC_INT.1.1
MAT_PAS.1	11	Archives nécessitant une climatisation pour leur conservation	PHY_01	CAR_AAR.1.1
MAT_PAS.1	11	Archives nécessitant une climatisation pour leur conservation	PHY_01	BPE_SEM.4.1
MAT_PAS.1	11	Archives nécessitant une climatisation pour leur conservation	MAT_03	BPE_SEM.1.1
MAT_PAS.1	11	Archives nécessitant une climatisation pour leur conservation	MAT_03	BMA_MAA.2.1
MAT_PAS.1	11	Archives nécessitant une climatisation pour leur conservation	PHY_01	BPE_SEM.2.1
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	BPE_ZOS.2.1
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	BPE_SEM.5.1
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	BPE_SEM.1.1
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	BCM_RLC.1.1
MAT_PAS.1	20	Absence d'inventaire des supports utilisés	MAT_06	BCM_RLC.1.1
MAT_PAS.1	20	Absence de sauvegarde des données contenues sur les supports	ORG_08	BGC_INT.1.1
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	BPE_ZOS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	CET_EGT.1.8
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	CET_EGT.1.9
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	CET_EGT.1.10
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	CET_EGT.2.3
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)	MAT_07	CGS_PPS.3.2
MAT_PAS.1	22	Présence de données résiduelles à l'insu de l'utilisateur de matériels ré-attribués ou mis au rebut	MAT_08	BGC_MSS.2.1
MAT_PAS.1	26	Absence de moyens permettant le contrôle d'innocuité des supports lors de leurs entrées dans l'organisme	ORG_06	BDM_SED.4.1
MAT_PAS.1	26	Absence de moyens permettant le contrôle d'innocuité des supports lors de leurs entrées dans l'organisme	ORG_06	BGC_PLM.1.1
MAT_PAS.1	26	Absence de moyens permettant le contrôle d'innocuité des supports lors de leurs entrées dans l'organisme	ORG_06	CGS_OML.1.3
MAT_PAS.1	26	Absence de moyens permettant le contrôle d'innocuité des supports lors de leurs entrées dans l'organisme	ORG_06	CGS_OML.1.1
MAT_PAS.1	28	Mauvaise condition de stockage	PHY_03	CIS_PSI.1.2
MAT_PAS.1	28	Mauvaise condition de stockage	PHY_03	CIS_PSI.1.1
MAT_PAS.1	28	Support non adapté à la durée de vie des données à archiver	MAT_04	CGS_ARC.1.1
MAT_PAS.1	28	Support non adapté à la durée de vie des données à archiver	MAT_04	CGS_ARC.1.2
MAT_PAS.1	29	Support non adapté à la durée de vie des données à archiver	MAT_03	BPE_SEM.1.1
MAT_PAS.1	29	Support non adapté à la durée de vie des données à archiver	MAT_03	BMA_MAA.2.1
MAT_PAS.1	29	Mauvaise condition de stockage	PHY_03	CIS_PSI.1.2
MAT_PAS.1	29	Mauvaise condition de stockage	PHY_03	CIS_PSI.1.1
MAT_PAS.1	30	Persistance involontaire des données sur les supports	ORG_09	BGC_MSS.2.1
MAT_PAS.1	30	Persistance involontaire des données sur les supports	ORG_09	BSP_FOU.1.1
MAT_PAS.1	30	Persistance involontaire des données sur les supports	ORG_09	FDP_RIP.1.1
MAT_PAS.1	30	Persistance involontaire des données sur les supports	ORG_09	FDP_RIP.2.1
MAT_PAS.1	30	Persistance involontaire des données sur les supports	ORG_09	BPE_SEM.6.1
MAT_PAS.1	32	Modification des équipements, des logiciels ou des procédures de sauvegarde sans prise en compte des anciennes sauvegardes ou archives	ORG_05	CGS_SVG.1.7
MAT_PAS.1	32	Support obsolète	ORG_13	BPE_SEM.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS.1	32	Modification des équipements, des logiciels ou des procédures de sauvegarde sans prise en compte des anciennes sauvegardes ou archives	ORG_05	CDO_SDC.1.2
MAT_PAS.1	32	Modification des équipements, des logiciels ou des procédures de sauvegarde sans prise en compte des anciennes sauvegardes ou archives	ORG_05	CGS_ARC.1.7
MAT_PAS.1	37	Absence de procédure et moyen de destruction	MAT_08	BGC_MSS.2.1
MAT_PAS.1	37	Absence de moyen de chiffrement	ORG_15	BDM_COC.2.1
MAT_PAS.1	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.2.1
MAT_PAS.1	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.1.1
MAT_PAS.1	38	Absence de responsabilité	PER_05	BSP_SPR.4.1
MAT_PAS.1	38	Absence de responsabilité	PER_05	BSP_SPR.1.1
MAT_PAS.1	38	Supports d'utilisation complexe ou peu ergonomique	MAT_11	BSP_FOU.2.1
MAT_PAS.1	39	Absence de protection physique	ORG_01	CIS_PSI.1.2
MAT_PAS.1	39	Absence de protection physique	ORG_01	CIS_PSI.1.1
MAT_PAS.1	40	Absence de protection des supports	ORG_30	BDM_COC.2.1
MAT_PAS.1	40	Absence de protection des supports	ORG_30	BPE_ZOS.1.1
MAT_PAS.1	40	Absence de protection des supports	ORG_30	BPE_ZOS.1.1
MAT_PAS.1	40	Absence de protection des supports	ORG_30	CGS_PPS.3.2
MAT_PAS.1	40	Absence de protection des supports	ORG_30	CET_EGT.2.3
MAT_PAS.1	40	Absence de protection des supports	ORG_30	BPE_ZOS.2.1
MAT_PAS.1	40	Absence de protection des supports	ORG_30	CGS_PPS.3.2
MAT_PAS.1	40	Absence de protection des supports	ORG_30	CET_EGT.2.3
MAT_PAS.1	40	Absence de protection des supports	ORG_30	BPE_ZOS.2.1

4.1.2.2 MAT_PAS.2 : Autres supports

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS.2	1	Supports originaux	MAT_02	BGC_INT.1.1
MAT_PAS.2	1	Supports originaux	MAT_02	CGS_SVG.1.1
MAT_PAS.2	1	Supports originaux	MAT_02	CGS_SVG.1.2
MAT_PAS.2	2	Supports originaux	MAT_02	CGS_SVG.1.1
MAT_PAS.2	2	Supports originaux	MAT_02	CGS_SVG.1.2
MAT_PAS.2	2	Supports originaux	MAT_02	BGC_INT.1.1
MAT_PAS.2	4	Supports originaux	MAT_02	CGS_SVG.1.2
MAT_PAS.2	4	Supports originaux	MAT_02	CGS_SVG.1.1
MAT_PAS.2	4	Supports originaux	MAT_02	BGC_INT.1.1
MAT_PAS.2	5	Supports originaux	MAT_02	CGS_SVG.1.2
MAT_PAS.2	5	Supports originaux	MAT_02	BGC_INT.1.1
MAT_PAS.2	5	Supports originaux	MAT_02	CGS_SVG.1.1
MAT_PAS.2	11	Archives nécessitant une climatisation pour leur conservation	PHY_01	CAR_AAR.1.1
MAT_PAS.2	11	Archives nécessitant une climatisation pour leur conservation	PHY_01	BPE_SEM.2.1
MAT_PAS.2	11	Archives nécessitant une climatisation pour leur conservation	PHY_01	BPE_SEM.4.1
MAT_PAS.2	11	Archives nécessitant une climatisation pour leur conservation	MAT_03	BMA_MAA.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
MAT_PAS.2	11	Archives nécessitant une climatisation pour leur conservation	MAT_03	BPE_SEM.1.1
MAT_PAS.2	18	Lecture de documents sensibles dans des lieux publics (observation des documents par des personnes extérieures…)	ORG_15	BDM_COC.2.1
MAT_PAS.2	20	Supports originaux	ORG_08	BGC_INT.1.1
MAT_PAS.2	32	Perte ou mauvaise gestion des documents originaux (contrats de support, licences…)	ORG_08	BGC_INT.1.1
MAT_PAS.2	39	Absence d'audit des procédures de contrôle d'accès physique	ORG_22	FAU_SAA.1.2
MAT_PAS.2	40	Absence d'audit des procédures de contrôle d'accès physique	ORG_22	FAU_SAA.1.2
MAT_PAS.2	41	Absence de procédure d'accès à l'information classifiée	ORG_15	BDM_COC.2.1

4.2 LOG : Logiciel

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	FIA_SOS.2.2
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	CGS_GMP.1.2
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	CGS_GMP.1.1
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	BMA_REU.2.1
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	BMA_MAS.4.1
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	FIA_SOS.2.1
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	FIA_SOS.1.1
LOG	18	Absence de dispositif de protège écran en cas d'inactivité	LOG_16	BMA_MAS.8.1
LOG	18	Absence de dispositif de protège écran en cas d'inactivité	LOG_16	CIS_ADL.1.1
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)	ORG_10	BMA_REU.1.1
LOG	18	Absence de dispositif de protège écran en cas d'inactivité	LOG_16	FTA_SSL.2.1
LOG	18	Absence de dispositif de protège écran en cas d'inactivité	LOG_16	BMA_MAS.7.1
LOG	18	Pas ou peu de changement de mot de passe d'accès au système ou à l'application	ORG_10	BMA_MAS.4.1
LOG	18	Absence de dispositif de protège écran en cas d'inactivité	LOG_16	FTA_SSL.3.1
LOG	18	Absence de dispositif de protège écran en cas d'inactivité	LOG_16	FTA_SSL.1.1
LOG	19	Possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie	LOG_08	BDM_SED.4.1
LOG	19	Possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie	LOG_08	CGS_PPS.2.3
LOG	19	Possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie	LOG_08	CGS_PPS.2.4
LOG	19	Absence de dispositif de contrôle d'accès en cas d'inactivité	LOG_13	FTA_SSL.1.1
LOG	19	Absence de dispositif de contrôle d'accès en cas d'inactivité	LOG_13	FTA_SSL.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG	19	Absence de dispositif de contrôle d'accès en cas d'inactivité	LOG_13	FTA_SSL.3.1
LOG	19	Absence de dispositif de contrôle d'accès en cas d'inactivité	LOG_13	BMA_MAS.7.1
LOG	19	Absence de dispositif de contrôle d'accès en cas d'inactivité	LOG_13	BMA_MAS.8.1
LOG	22	Présence de données résiduelles utilisées par les logiciels	MAT_08	BGC_INT.1.1
LOG	22	Présence de données résiduelles utilisées par les logiciels	MAT_08	CGS_SVG.1.2
LOG	23	Absence de vérification des accès partagés accordés	LOG_13	BMA_MAS.3.1
LOG	23	Absence de vérification des accès partagés accordés	LOG_13	FIA_UAU.7.1
LOG	23	Procédures de gestion des privilèges d'accès trop lourde à opérer	ORG_36	CGS_PAI.1.4
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_03	BDM_SED.2.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_03	BGC_PRE.2.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_08	CGS_PPS.2.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_08	BDM_SED.4.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_08	BDM_SED.3.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_08	BDM_SED.1.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_03	BDM_SED.1.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_08	BGC_PRS.2.1
LOG	24	Récupération de logiciels depuis un moyen de collecte non authentifié	LOG_08	BCO_RPS.2.1
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_03	BDM_SED.4.1
LOG	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_38	BDM_SED.4.1
LOG	26	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_38	CGS_PPS.2.3
LOG	30	Absence de prise en compte dans la définition des exigences d'un projet des situations particulières plaçant le système dans des conditions aux limites	LOG_14	FRU_FLT.1.1
LOG	30	Absence de filtre protégeant le système contre un engorgement	LOG_14	FRU_FLT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG	30	Application nécessitant des ressources informatiques non adaptée au matériel (ex.: manque de mémoire vive)	MAT_09	CAR_AAR.1.1
LOG	30	Application nécessitant des ressources informatiques non adaptée au matériel (ex.: manque de mémoire vive)	MAT_09	BDM_ESS.1.1
LOG	30	Consommation inutile de ressources	LOG_14	CAR_AAR.1.1
LOG	30	Absence de qualification des développements dans un contexte représentatif de l'exploitation	LOG_06	BGC_PLM.1.1
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_06	BSP_FOU.1.1
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_06	BSP_FOU.2.1
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_06	CDO_APP.1.1
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_06	CDO_APP.1.2
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	ORG_14	BSP_FOU.1.1
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	ORG_14	BSP_FOU.2.1
LOG	31	Absence de compte rendu des opérations de maintenance	LOG_08	BCO_RPS.2.1
LOG	31	Absence de procédure de synchronisation des horloges	LOG_10	FPT_STM.1.1
LOG	31	Absence de procédure de maintenance	LOG_09	BGC_PRE.1.1
LOG	31	Absence de procédure de maintenance	LOG_09	CDO_APP.1.1
LOG	31	Absence de procédure de maintenance	LOG_09	CDO_APP.1.2
LOG	31	Absence de remontée d'information pour le traitement centralisé des dysfonctionnements	LOG_15	CET_EGT.1.6
LOG	31	Absence de procédure de qualification avant toute installation ou mise à jour	LOG_06	BGC_PLM.1.1
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	ORG_14	CDO_APP.1.1
LOG	31	Absence de compte rendu des opérations de maintenance	LOG_03	BDM_SED.2.1
LOG	31	Possibilité de mal configurer, installer ou modifier le système d'exploitation	LOG_04	FMT_MSA.3.1
LOG	31	Possibles effets de bord liés à la mise à jour d'un composant logiciel	LOG_02	BDM_SED.5.1
LOG	31	Possibles effets de bord liés à la mise à jour d'un composant logiciel	LOG_02	BDM_SED.4.1
LOG	31	Possibles effets de bord liés à la mise à jour d'un composant logiciel	LOG_02	BDM_SED.3.1
LOG	31	Possibles effets de bord liés à la mise à jour d'un composant logiciel	LOG_02	BDM_SED.2.1
LOG	31	Possibles effets de bord liés à la mise à jour d'un composant logiciel	LOG_02	BDM_SED.1.1
LOG	31	Possibles effets de bord liés à la mise à jour d'un composant logiciel	LOG_02	BGC_PRS.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG	31	Absence ou erreur de gestion en configuration des composants logiciels (ex: application d'un patch UK non adapté à une version FR)	LOG_08	BGC_PRS.2.1
LOG	31	Absence de procédure de synchronisation des horloges	LOG_10	BMA_SAS.3.1
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	ORG_14	CDO_APP.1.2
LOG	31	Absence de conservation des traces des traitements	LOG_10	BMA_SAS.1.1
LOG	32	Absence de documentation à jour	ORG_28	CDO_APP.1.1
LOG	32	Absence de documentation à jour	ORG_28	CDO_APP.1.3
LOG	32	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_12	CDO_APP.1.1
LOG	32	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_12	CDO_APP.1.2
LOG	32	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_12	BSP_FOU.1.1
LOG	32	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_12	BSP_FOU.2.1
LOG	32	Absence de procédure de secours	ORG_24	CGS_GSS.2.1
LOG	32	Absence de procédure de secours	ORG_24	CGS_GSS.2.2
LOG	32	Logiciels obsolètes	LOG_09	CEI_CDT.1.2
LOG	32	Logiciels spécifiques	ORG_09	CDO_APP.1.1
LOG	32	Absence de compte rendu des opérations de maintenance	LOG_03	CET_EIP.1.5
LOG	32	Logiciels spécifiques	ORG_09	CDO_APP.1.2
LOG	32	Logiciels spécifiques	ORG_09	BGC_PRS.2.1
LOG	32	Logiciels obsolètes	LOG_09	CEI_CDT.1.1
LOG	32	Absence de procédure de maintenance	LOG_09	CDO_APP.1.2
LOG	32	Absence de procédure de maintenance	LOG_09	CDO_APP.1.1
LOG	32	Absence de compte rendu des opérations de maintenance	LOG_03	BDM_SED.2.1
LOG	32	Absence de compte rendu des opérations de maintenance	LOG_03	BCO_RPS.2.1
LOG	32	Absence de compte rendu des opérations de maintenance	LOG_03	CET_EIP.1.4
LOG	32	Absence de compte rendu des opérations de maintenance	LOG_03	CET_EIP.1.6
LOG	32	Absence de conservation des traces des traitements et des modifications	LOG_03	BMA_SAS.1.1
LOG	32	Absence de conservation des traces des traitements et des modifications	LOG_03	BGC_PRE.2.2
LOG	32	Absence de procédure de retour arrière en cas d'anomalie lors d'une modification	LOG_02	BGC_PRE.2.1
LOG	32	Absence de procédure de retour arrière en cas d'anomalie lors d'une modification	LOG_02	CDO_SDC.1.2
LOG	32	Absence de procédure de retour arrière en cas d'anomalie lors d'une modification	LOG_02	CGS_GMA.6.1
LOG	32	Logiciels à configurations non évolutives	LOG_06	BGC_PLM.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG	32	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PLM.1.1
LOG	32	Absence de compte rendu des opérations de maintenance	LOG_03	CET_EIP.1.3
LOG	32	Absence de procédure de maintenance	LOG_09	BGC_PRE.1.1
LOG	32	Absence de procédure de secours	ORG_24	BGC_PRE.1.1
LOG	33	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BDM_SED.4.1
LOG	33	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	CGS_PPS.2.4
LOG	33	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BMA_MAS.3.1
LOG	33	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	FIA_UAU.7.1
LOG	33	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	BMA_MAS.3.1
LOG	33	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	FIA_UAU.7.1
LOG	33	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	CGS_GLI.1.1
LOG	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité...)	LOG_11	CGS_GDH.1.2
LOG	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité...)	LOG_11	CGS_GDH.2.1
LOG	34	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	CGS_GLI.1.1
LOG	34	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	BCM_RLC.1.1
LOG	36	Absence de contrôle de l'intégrité des données	LOG_01	FDP_SDI.1/2.1
LOG	36	Absence de procédure et de dispositif d'habilitation à la modification des données	LOG_11	CGS_GDH.1.2
LOG	36	Absence de procédure et de dispositif d'habilitation à la modification des données	LOG_11	CGS_GDH.2.1
LOG	36	Absence de contrôle de l'intégrité des données	LOG_01	FDP_SDI.2.1
LOG	39	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
LOG	40	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
LOG	41	Absence de politique d'audit	ORG_22	FAU_SAA.1.2

4.2.1 LOG_OS : Système d'exploitation

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_OS	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_OS	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_OS	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_OS	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_OS	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_OS	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_OS	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_OS	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_OS	19	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.2.1
LOG_OS	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application	ORG_10	CGS_GMP.1.1
LOG_OS	19	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.1.2
LOG_OS	26	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_08	BCO_RPS.2.1
LOG_OS	26	Possibilité de créer ou modifier des commandes systèmes	LOG_08	BCO_RPS.2.1
LOG_OS	26	Possibilité d'effacer, de modifier ou d'installer des nouveaux programmes	LOG_08	BCO_RPS.2.1
LOG_OS	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1
LOG_OS	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.4.1
LOG_OS	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
LOG_OS	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
LOG_OS	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BMA_MAR.4.1
LOG_OS	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
LOG_OS	26	Récupération de logiciels depuis un moyen de collecte non authentifié	LOG_06	BGC_PLM.1.1
LOG_OS	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
LOG_OS	26	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_11	CGS_GDH.2.1
LOG_OS	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
LOG_OS	26	Possibilité d'administrer le système à distance	RES_06	BGC_PLM.1.1
LOG_OS	26	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
LOG_OS	26	La couche SNMP est activée	LOG_12	FAU_SAA.2.3
LOG_OS	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
LOG_OS	26	Utilisation d'un système d'exploitation standard pour lequel des attaques logiques ont déjà été réalisées	LOG_06	CGS_PPS.2.4
LOG_OS	26	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…	LOG_11	CGS_GDH.1.2
LOG_OS	26	Utilisation d'un système d'exploitation standard pour lequel des attaques logiques ont déjà été réalisées	LOG_06	CGS_PPS.2.4
LOG_OS	28	Absence de fonction de diagnostic pour la prévention des pannes matérielles	LOG_14	FRU_FLT.1.1
LOG_OS	29	Absence de fonction de diagnostic pour la prévention des pannes matérielles	LOG_14	FRU_FLT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2
LOG_OS	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
LOG_OS	31	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PLM.1.1
LOG_OS	33	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées	LOG_12	FAU_SAA.2.3
LOG_OS	34	Système d'exploitation attractif ou "grand public"	ORG_04	BDM_SFS.3.1
LOG_OS	34	Système d'exploitation attractif ou "grand public"	ORG_04	CGS_GLI.1.4
LOG_OS	34	Possibilité de copier facilement les distributions des systèmes d'exploitation propriétaires	ORG_04	BDM_SFS.3.1
LOG_OS	34	Possibilité de copier facilement les distributions des systèmes d'exploitation propriétaires	ORG_04	CGS_GLI.1.4
LOG_OS	34	Possibilité de copier facilement les distributions des systèmes d'exploitation propriétaires	ORG_04	CGS_GLI.2.1
LOG_OS	34	Système d'exploitation attractif ou "grand public"	ORG_04	CGS_GLI.2.1
LOG_OS	35	Possibilité que les systèmes fonctionnent avec des systèmes d'exploitation copiés illicitement ou contrefaits	ORG_04	BCO_CEL.2.1
LOG_OS	35	Possibilité que les systèmes fonctionnent avec des systèmes d'exploitation copiés illicitement ou contrefaits	LOG_07	BCM_RLC.1.1
LOG_OS	35	Possibilité que les systèmes fonctionnent avec des systèmes d'exploitation copiés illicitement ou contrefaits	LOG_08	BCM_RLC.1.1
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.2
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.1.1
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.2
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.1.1
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.2.1
LOG_OS	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
LOG_OS	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.1
LOG_OS	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
LOG_OS	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
LOG_OS	36	La couche SNMP est activée	LOG_12	FAU_SAA.2.3
LOG_OS	36	Possibilité d'administrer le système à distance	RES_06	BDM_COC.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	36	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
LOG_OS	36	Le système d'exploitation permet d'accéder à des données (base de données…)	LOG_11	CGS_GDH.2.1
LOG_OS	36	Le système d'exploitation permet d'accéder à des données (base de données…)	LOG_11	CGS_GDH.1.2
LOG_OS	36	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées	LOG_12	FAU_SAA.2.3
LOG_OS	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1
LOG_OS	36	Aucune vérification du système d'exploitation n'est faite avant l'installation	LOG_06	BGC_PRS.2.1
LOG_OS	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.4.1
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.1
LOG_OS	36	Absence de restriction sur les points d'entrée dans le logiciel	LOG_13	FIA_UAU.7.1
LOG_OS	36	Absence de restriction sur les points d'entrée dans le logiciel	LOG_13	BMA_MAS.3.1
LOG_OS	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BMA_MAR.4.1
LOG_OS	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
LOG_OS	36	Aucune vérification du système d'exploitation n'est faite avant l'installation	LOG_06	BDM_SED.4.1
LOG_OS	36	Aucune vérification du système d'exploitation n'est faite avant l'installation	LOG_06	CGS_OML.1.1
LOG_OS	36	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG_OS	37	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_SEP.1.1
LOG_OS	37	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_RVM.1.1
LOG_OS	37	Absence de dispositif de chiffrement	RES_02	BDM_COC.2.1
LOG_OS	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	CGS_PPS.2.4
LOG_OS	37	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	CGS_PPS.1.1
LOG_OS	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	CGS_PPS.2.3
LOG_OS	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BDM_SED.4.1
LOG_OS	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	CGS_PPS.2.3
LOG_OS	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	CGS_PPS.2.4
LOG_OS	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	BDM_SED.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.1.2
LOG_OS	38	Utilisation non intuitive du logiciel	LOG_17	CGS_PPS.2.3
LOG_OS	38	Insuffisance de compétence	ORG_14	BSP_FOU.2.1
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.3.3
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.3.2
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.1.1
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.2.1
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.2.2
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.2.3
LOG_OS	38	Insuffisance de compétence	ORG_14	BSP_FOU.1.1
LOG_OS	38	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	ORG_14	BSP_FOU.2.1
LOG_OS	38	Absence de support accessible	ORG_27	CGS_GSU.3.1
LOG_OS	38	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels	PER_06	BSP_FOU.2.1
LOG_OS	39	Les mots de passe saisis pour accéder au système d'exploitation sont déchiffrables	ORG_10	BMA_MAS.4.1
LOG_OS	39	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_SEP.1.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FMT_MOF.1.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_06	BDM_COC.4.1
LOG_OS	39	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
LOG_OS	39	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2
LOG_OS	39	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	FAU_GEN.1.1
LOG_OS	39	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	FAU_GEN.1.2
LOG_OS	39	Les logs ou journaux du système d'exploitation sont modifiables par tous	LOG_11	CGS_GDH.2.1
LOG_OS	39	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	BMA_SAS.1.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FPT_ITA.1.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FTA_TSE.1.1
LOG_OS	39	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
LOG_OS	39	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_RVM.1.1
LOG_OS	39	Les logs ou journaux du système d'exploitation sont modifiables par tous	LOG_11	CGS_GDH.1.2
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.3.2
LOG_OS	39	Le système d'exploitation permet l'ouverture de session sans mot de passe	LOG_13	BMA_MAS.3.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.1
LOG_OS	39	Le système d'exploitation permet l'établissement de connexions anonymes	LOG_13	BMA_MAS.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	39	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
LOG_OS	39	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")	LOG_11	CGS_GDH.2.1
LOG_OS	39	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")	LOG_11	CGS_GDH.1.2
LOG_OS	39	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées	LOG_12	FAU_SAA.2.3
LOG_OS	39	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG_OS	39	La couche SNMP est activée	LOG_12	FAU_SAA.2.3
LOG_OS	39	La base de mots de passe du système d'exploitation est déchiffrable	ORG_10	BMA_MAS.4.1
LOG_OS	39	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
LOG_OS	39	Le système d'exploitation permet l'établissement de connexions anonymes	LOG_13	FIA_UAU.7.1
LOG_OS	39	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MOF.1.1
LOG_OS	39	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.1.1
LOG_OS	39	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
LOG_OS	39	Le système d'exploitation permet l'ouverture de session sans mot de passe	LOG_13	FIA_UAU.7.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.2
LOG_OS	39	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
LOG_OS	39	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	CGS_PPS.2.4
LOG_OS	39	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.2.1
LOG_OS	39	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.1.1
LOG_OS	39	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.3.2
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.2.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.1.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.1.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	CAR_PAR.1.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.2.3
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.1
LOG_OS	39	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.2
LOG_OS	39	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	CGS_PPS.1.1
LOG_OS	40	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	FAU_GEN.1.1
LOG_OS	40	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	40	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
LOG_OS	40	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	BMA_SAS.1.1
LOG_OS	40	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")	LOG_11	CGS_GDH.2.1
LOG_OS	40	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")	LOG_11	CGS_GDH.1.2
LOG_OS	40	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG_OS	40	La couche SNMP est activée	LOG_12	FAU_SAA.2.3
LOG_OS	40	La base de mots de passe du système d'exploitation est déchiffrable	ORG_10	BMA_MAS.4.1
LOG_OS	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
LOG_OS	40	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	FAU_GEN.1.2
LOG_OS	40	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées	LOG_12	FAU_SAA.2.3
LOG_OS	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
LOG_OS	40	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	CAR_AAR.1.1
LOG_OS	40	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_SEP.1.1
LOG_OS	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
LOG_OS	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
LOG_OS	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
LOG_OS	40	Possibilité d'administrer le système à distance	RES_06	BDM_COC.4.1
LOG_OS	40	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
LOG_OS	40	Les mots de passe saisis pour accéder au système d'exploitation sont déchiffrables	ORG_10	BMA_MAS.4.1
LOG_OS	40	Les logs ou journaux du système d'exploitation sont modifiables par tous	LOG_11	CGS_GDH.2.1
LOG_OS	40	Les logs ou journaux du système d'exploitation sont modifiables par tous	LOG_11	CGS_GDH.1.2
LOG_OS	40	Le système d'exploitation permet l'ouverture de session sans mot de passe	LOG_13	FIA_UAU.7.1
LOG_OS	40	Le système d'exploitation permet l'ouverture de session sans mot de passe	LOG_13	BMA_MAS.3.1
LOG_OS	40	Le système d'exploitation permet l'établissement de connexions anonymes	LOG_13	BMA_MAS.3.1
LOG_OS	40	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	CGS_PPS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	40	Le système d'exploitation permet l'établissement de connexions anonymes	LOG_13	FIA_UAU.7.1
LOG_OS	40	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_RVM.1.1
LOG_OS	40	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
LOG_OS	40	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
LOG_OS	41	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	CGS_PPS.1.1
LOG_OS	41	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
LOG_OS	41	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
LOG_OS	41	Le système d'exploitation permet l'ouverture de session sans mot de passe	LOG_13	FIA_UAU.7.1
LOG_OS	41	Les mots de passe saisis pour accéder au système d'exploitation sont déchiffrables	ORG_10	BMA_MAS.4.1
LOG_OS	41	La base de mots de passe du système d'exploitation est déchiffrable	ORG_10	BMA_MAS.4.1
LOG_OS	41	Possibilité d'administrer le système à distance	RES_06	BDM_COC.4.1
LOG_OS	41	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
LOG_OS	41	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	FAU_GEN.1.1
LOG_OS	41	Les logs ou journaux du système d'exploitation sont modifiables par tous	LOG_11	CGS_GDH.1.2
LOG_OS	41	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_RVM.1.1
LOG_OS	41	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
LOG_OS	41	Les logs ou journaux du système d'exploitation sont modifiables par tous	LOG_11	CGS_GDH.2.1
LOG_OS	41	La couche SNMP est activée	LOG_12	FAU_SAA.2.3
LOG_OS	41	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG_OS	41	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées	LOG_12	FAU_SAA.2.3
LOG_OS	41	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")	LOG_11	CGS_GDH.1.2
LOG_OS	41	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")	LOG_11	CGS_GDH.2.1
LOG_OS	41	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	BMA_SAS.1.1
LOG_OS	41	Le système d'exploitation permet l'établissement de connexions anonymes	LOG_13	BMA_MAS.3.1
LOG_OS	41	Le système d'exploitation permet l'établissement de connexions anonymes	LOG_13	FIA_UAU.7.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_OS	41	Le système d'exploitation permet l'ouverture de session sans mot de passe	LOG_13	BMA_MAS.3.1
LOG_OS	41	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)	LOG_08	FPT_SEP.1.1
LOG_OS	41	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
LOG_OS	41	Le système d'exploitation ne journalise pas les logs ou les événements systèmes	LOG_15	FAU_GEN.1.2
LOG_OS	41	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
LOG_OS	41	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
LOG_OS	41	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.4.1
LOG_OS	41	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2
LOG_OS	41	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	CAR_AAR.1.1

4.2.2 LOG_SRV : Logiciel de service, maintenance ou administration

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_SRV	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_SRV	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_SRV	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_SRV	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_SRV	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_SRV	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_SRV	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_SRV	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_SRV	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_SRV	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_SRV	19	Pas ou peu de changement de mot de passe d'accès aux logiciels de support	ORG_10	CGS_GMP.1.1
LOG_SRV	24	Absence de conservation des traces des activités	LOG_10	BMA_SAS.1.1
LOG_SRV	24	Absence de moyen sûr d'identification	LOG_13	BMA_MAS.3.1
LOG_SRV	24	Absence de moyen sûr d'identification	LOG_13	FIA_UAU.7.1
LOG_SRV	26	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.2.1
LOG_SRV	26	Possibilité de modifier, d'altérer le logiciel	LOG_01	FPT_ITI.1/2.2
LOG_SRV	26	Utilisation de logiciels non évalués	LOG_06	BGC_PLM.1.1
LOG_SRV	26	Possibilité de modifier, d'altérer le logiciel	LOG_01	FPT_ITT.3.1
LOG_SRV	26	Possibilité de modifier, d'altérer le logiciel	LOG_01	FPT_ITT.3.2
LOG_SRV	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_SRV	26	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.1.2
LOG_SRV	28	Absence de fonction de diagnostic pour la prévention des pannes matérielles	LOG_14	FRU_FLT.1.1
LOG_SRV	29	Absence de fonction de diagnostic pour la prévention des pannes matérielles	LOG_14	FRU_FLT.1.1
LOG_SRV	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
LOG_SRV	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2
LOG_SRV	31	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PLM.1.1
LOG_SRV	33	Utilisation partagée d'identifiant de connexion	LOG_11	CGS_GDH.2.1
LOG_SRV	33	Utilisation partagée d'identifiant de connexion	LOG_11	CGS_GDH.1.2
LOG_SRV	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.2.1
LOG_SRV	34	Logiciels attractifs ou "grand public"	ORG_04	BDM_SFS.3.1
LOG_SRV	34	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.1.4
LOG_SRV	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.1.4
LOG_SRV	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	BDM_SFS.3.1
LOG_SRV	34	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.2.1
LOG_SRV	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.1.4
LOG_SRV	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	CGS_GLI.1.1
LOG_SRV	35	Logiciels attractifs ou "grand public"	ORG_04	BDM_SFS.3.1
LOG_SRV	35	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.1.4
LOG_SRV	35	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.2.1
LOG_SRV	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	BCM_RLC.1.1
LOG_SRV	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	BDM_SFS.3.1
LOG_SRV	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.2.1
LOG_SRV	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)	LOG_11	CGS_GDH.1.2
LOG_SRV	36	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG_SRV	36	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PLM.1.1
LOG_SRV	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
LOG_SRV	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)	LOG_11	CGS_GDH.2.1
LOG_SRV	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	FIA_UAU.7.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_SRV	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	CGS_PPS.2.4
LOG_SRV	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BDM_SED.4.1
LOG_SRV	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	FIA_UAU.7.1
LOG_SRV	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	BMA_MAS.3.1
LOG_SRV	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BMA_MAS.3.1
LOG_SRV	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	BMA_MAS.3.1
LOG_SRV	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	FIA_UAU.7.1
LOG_SRV	37	Absence de dispositif de chiffrement	RES_02	BDM_COC.2.1
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.2
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.1
LOG_SRV	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.1.1
LOG_SRV	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.2.1
LOG_SRV	38	Absence de responsabilité	ORG_14	BSP_SPR.4.1
LOG_SRV	38	Absence de responsabilité	ORG_14	BSP_SPR.1.1
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.3
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.2
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.3
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.1
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.2
LOG_SRV	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.1
LOG_SRV	38	Logiciel d'utilisation complexe	LOG_17	CGS_PPS.2.3
LOG_SRV	39	Absence de sauvegarde des journaux d'événements	ORG_08	CGS_SVG.1.2
LOG_SRV	39	Absence de sauvegarde des journaux d'événements	ORG_08	CGS_SVG.1.2
LOG_SRV	39	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	BMA_MAS.3.1
LOG_SRV	39	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
LOG_SRV	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_SRV	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_SRV	39	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	FIA_UAU.7.1
LOG_SRV	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_SRV	40	Absence de sauvegarde des journaux d'événements	ORG_08	BGC_INT.1.1
LOG_SRV	40	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	BMA_MAS.3.1
LOG_SRV	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_SRV	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_SRV	40	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	FIA_UAU.7.1
LOG_SRV	41	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	BMA_MAS.3.1
LOG_SRV	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_SRV	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_SRV	41	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	FIA_UAU.7.1
LOG_SRV	41	Absence de sauvegarde des journaux d'événements	ORG_08	BGC_INT.1.1
LOG_SRV	41	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1

4.2.3 LOG_STD : Progiciel ou logiciel standard

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_STD	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_STD	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_STD	1	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_STD	1	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_STD	2	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_STD	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_STD	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_STD	2	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_STD	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_STD	3	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_STD	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_STD	3	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_STD	4	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_STD	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_STD	4	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_STD	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_STD	5	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_STD	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_STD	5	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_STD	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_STD	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application	ORG_10	CGS_GMP.1.1
LOG_STD	19	Absence de protection des journaux récoltant la trace des activités	ORG_15	BDM_COC.2.1
LOG_STD	24	Absence de conservation des traces des activités	LOG_10	BMA_SAS.1.1
LOG_STD	24	Absence de moyen sûr d'identification	LOG_13	FIA_UAU.7.1
LOG_STD	24	Absence de moyen sûr d'identification	LOG_13	BMA_MAS.3.1
LOG_STD	26	Utilisation de logiciels non évalués	LOG_06	BGC_PLM.1.1
LOG_STD	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_STD	26	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.1.2
LOG_STD	26	Possibilité de modifier, d'altérer le logiciel	LOG_01	FPT_TST.1.2
LOG_STD	26	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.2.1
LOG_STD	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
LOG_STD	31	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PLM.1.1
LOG_STD	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2
LOG_STD	33	Utilisation partagée d'identifiant de connexion	LOG_11	CGS_GDH.2.1
LOG_STD	33	Utilisation partagée d'identifiant de connexion	LOG_11	CGS_GDH.1.2
LOG_STD	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.2.1
LOG_STD	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.1.4
LOG_STD	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	BDM_SFS.3.1
LOG_STD	34	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.2.1
LOG_STD	34	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.1.4
LOG_STD	34	Logiciels attractifs ou "grand public"	ORG_04	BDM_SFS.3.1
LOG_STD	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.1.4
LOG_STD	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	BDM_SFS.3.1
LOG_STD	35	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.2.1
LOG_STD	35	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.1.4
LOG_STD	35	Logiciels attractifs ou "grand public"	ORG_04	BDM_SFS.3.1
LOG_STD	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	CGS_GLI.1.1
LOG_STD	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	BCM_RLC.1.1
LOG_STD	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.2.1
LOG_STD	36	Absence de restriction sur les points d'entrée dans le logiciel	LOG_13	FIA_UAU.7.1
LOG_STD	36	Absence de restriction sur les points d'entrée dans le logiciel	LOG_13	BMA_MAS.3.1
LOG_STD	36	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG_STD	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
LOG_STD	36	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PLM.1.1
LOG_STD	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)	LOG_11	CGS_GDH.1.2
LOG_STD	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)	LOG_11	CGS_GDH.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_STD	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	BMA_MAS.3.1
LOG_STD	37	Absence de dispositif de chiffrement	RES_02	BDM_COC.2.1
LOG_STD	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	FIA_UAU.7.1
LOG_STD	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	BMA_MAS.3.1
LOG_STD	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	FIA_UAU.7.1
LOG_STD	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BMA_MAS.3.1
LOG_STD	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	FIA_UAU.7.1
LOG_STD	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BDM_SED.4.1
LOG_STD	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	CGS_PPS.2.4
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.1
LOG_STD	38	Logiciel d'utilisation complexe	LOG_17	CGS_PPS.2.3
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.1
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.2
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.1
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.3
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.2
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.3
LOG_STD	38	Absence de responsabilité	ORG_14	BSP_SPR.1.1
LOG_STD	38	Absence de responsabilité	ORG_14	BSP_SPR.4.1
LOG_STD	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.2.1
LOG_STD	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.1.1
LOG_STD	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.2
LOG_STD	39	Absence de sauvegarde des journaux d'événements	ORG_08	CGS_SVG.1.2
LOG_STD	39	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	CGS_PPS.2.4
LOG_STD	39	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
LOG_STD	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_STD	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_STD	40	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	CAR_AAR.1.1
LOG_STD	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_STD	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
LOG_STD	40	Absence de sauvegarde des journaux d'événements	ORG_08	BGC_INT.1.1
LOG_STD	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_STD	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_STD	41	Absence de sauvegarde des journaux d'événements	ORG_08	BGC_INT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_STD	41	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
LOG_STD	41	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	CAR_AAR.1.1
LOG_STD	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2

4.2.4 LOG_APP : Application métier

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_APP	19	Absence de protection des journaux récoltant la trace des activités	ORG_15	BDM_COC.2.1
LOG_APP	24	Absence de moyen sûr d'identification	LOG_13	BMA_MAS.3.1
LOG_APP	24	Absence de moyen sûr d'identification	LOG_13	FIA_UAU.7.1
LOG_APP	24	Absence de conservation des traces des activités	LOG_10	BMA_SAS.1.1
LOG_APP	26	Utilisation de logiciels non évalués	LOG_06	BDM_SED.4.1
LOG_APP	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
LOG_APP	26	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.1.2
LOG_APP	26	Absence de protection contre l'usage de privilèges avancés	LOG_11	CGS_GDH.2.1
LOG_APP	26	Utilisation de logiciels non évalués	LOG_06	BDM_SFS.1.1
LOG_APP	26	Possibilité de modifier, d'altérer le logiciel	LOG_01	FPT_TST.1.2
LOG_APP	31	Absence de documentation à jour	ORG_28	CDO_APP.1.1
LOG_APP	31	Absence de documentation à jour	ORG_28	CDO_APP.1.3
LOG_APP	33	Utilisation partagée d'identifiant de connexion	LOG_11	CGS_GDH.2.1
LOG_APP	33	Utilisation partagée d'identifiant de connexion	LOG_11	CGS_GDH.1.2
LOG_APP	34	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.2.1
LOG_APP	34	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.1.4
LOG_APP	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.1.4
LOG_APP	34	Logiciels attractifs ou "grand public"	ORG_04	BDM_SFS.3.1
LOG_APP	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.2.1
LOG_APP	34	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	BDM_SFS.3.1
LOG_APP	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.2.1
LOG_APP	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	CGS_GLI.1.4
LOG_APP	35	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.1.4
LOG_APP	35	Possibilité de copier facilement des logiciels ou progiciels	ORG_04	BDM_SFS.3.1
LOG_APP	35	Logiciels attractifs ou "grand public"	ORG_04	CGS_GLI.2.1
LOG_APP	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	CGS_GLI.1.1
LOG_APP	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation	LOG_07	BCM_RLC.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_APP	35	Logiciels attractifs ou "grand public"	ORG_04	BDM_SFS.3.1
LOG_APP	36	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
LOG_APP	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)	LOG_11	CGS_GDH.2.1
LOG_APP	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
LOG_APP	36	Absence de restriction sur les points d'entrée dans le logiciel	LOG_13	BMA_MAS.3.1
LOG_APP	36	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PLM.1.1
LOG_APP	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)	LOG_11	CGS_GDH.1.2
LOG_APP	36	Absence de restriction sur les points d'entrée dans le logiciel	LOG_13	FIA_UAU.7.1
LOG_APP	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BDM_SED.4.1
LOG_APP	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	CGS_PPS.2.4
LOG_APP	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	FIA_UAU.7.1
LOG_APP	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_08	BMA_MAS.3.1
LOG_APP	37	Absence de dispositif de chiffrement	RES_02	BDM_COC.2.1
LOG_APP	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	BMA_MAS.3.1
LOG_APP	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)	LOG_13	FIA_UAU.7.1
LOG_APP	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	BMA_MAS.3.1
LOG_APP	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation	LOG_13	FIA_UAU.7.1
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.3
LOG_APP	38	Absence de validation des données d'entrées (de saisie)	LOG_17	CGS_PPS.2.3
LOG_APP	38	Absence de procédure de tests et de réception conforme aux spécifications	LOG_06	BGC_PLM.1.1
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.2
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.1
LOG_APP	38	Absence de documentation explicite sur les systèmes applicatifs	ORG_28	CDO_APP.1.1
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.2
LOG_APP	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.2.1
LOG_APP	38	Absence de responsabilité	ORG_14	BSP_SPR.4.1
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.3
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.1
LOG_APP	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.1.1
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_APP	38	Absence de responsabilité	ORG_14	BSP_SPR.1.1
LOG_APP	38	Application d'utilisation complexe	LOG_17	CGS_PPS.2.3
LOG_APP	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.1
LOG_APP	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_APP	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_APP	39	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
LOG_APP	39	Absence de sauvegarde des journaux d'événements	ORG_08	CGS_SVG.1.2
LOG_APP	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
LOG_APP	40	Absence de sauvegarde des journaux d'événements	ORG_08	BGC_INT.1.1
LOG_APP	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
LOG_APP	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_APP	41	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
LOG_APP	41	Absence de sauvegarde des journaux d'événements	ORG_08	BGC_INT.1.1
LOG_APP	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
LOG_APP	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1

4.2.4.1 LOG_APP .1 : Application métier standard

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_APP.1	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_APP.1	1	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_APP.1	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_APP.1	2	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_APP.1	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_APP.1	3	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_APP.1	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_APP.1	4	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_APP.1	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.3
LOG_APP.1	5	Exemplaire unique des contrats de licence	LOG_07	CGS_GLI.1.2
LOG_APP.1	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application	ORG_10	CGS_GMP.1.1

4.2.4.2 LOG_APP .2 : Application métier spécifique

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_APP.2	1	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_APP.2	1	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_APP.2	2	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_APP.2	2	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_APP.2	3	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_APP.2	3	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_APP.2	4	Applications uniques développées en interne	MAT_02	BGC_INT.1.1
LOG_APP.2	4	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_APP.2	5	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_APP.2	5	Applications uniques développées en interne	MAT_02	BGC_INT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
LOG_APP.2	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application	ORG_10	CGS_GMP.1.1
LOG_APP.2	20	Applications uniques développées en interne	MAT_02	CGS_SVG.1.1
LOG_APP.2	20	Applications uniques développées en interne	MAT_02	CGS_SVG.1.2
LOG_APP.2	20	Applications uniques développées en interne	MAT_02	BGC_INT.1.1

4.3 RES : Réseau

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	BPE_ZOS.2.1
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	BPE_SEM.1.1
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	CET_EGT.2.3
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	BPE_ZOS.1.1
RES	6	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BPE_SEM.1.1
RES	6	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BMA_MAA.2.1
RES	7	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BPE_SEM.1.1
RES	7	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BMA_MAA.2.1
RES	8	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BMA_MAA.2.1
RES	8	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BPE_SEM.1.1
RES	9	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BMA_MAA.2.1
RES	9	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BPE_SEM.1.1
RES	10	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BMA_MAA.2.1
RES	10	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)	MAT_03	BPE_SEM.1.1
RES	17	Absence de prise en compte des règles d'installation	MAT_14	CGS_OML.1.1
RES	25	Possibilité de pose d'éléments matériels additionnels pour stocker, transmettre ou altérer (ex: keylogger physique)	RES_01	BGC_PLM.1.1
RES	25	Possibilité de pose d'une dérivation de circuit	RES_01	BGC_PLM.1.1
RES	28	Défaut de maintenance	ORG_27	CGS_GMA.1.2
RES	28	Défaut de maintenance	ORG_27	CGS_GMA.2.1
RES	28	Défaut de maintenance	ORG_27	CET_EIP.1.3
RES	33	Les équipements permettent d'utiliser les ressources du système depuis l'extérieur	RES_01	BMA_MAR.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES	33	Les équipements sont connectés à des réseaux externes	RES_01	BPE_SEM.1.1
RES	33	Les équipements permettent d'utiliser les ressources du système depuis l'extérieur	RES_01	BMA_MAR.4.1
RES	33	Les équipements utilisés permettent un autre usage que celui qui est prévu	RES_06	BMA_GAU.2.1
RES	33	Les équipements sont accessibles à tous	RES_01	BPE_SEM.1.1
RES	33	Les équipements sont connectés à des réseaux externes	RES_01	FTA_TAB.1.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BGC_PRE.4.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BPE_SEM.1.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BPE_ZOS.2.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BMA_EMA.1.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BMA_MAA.1.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BMA_MAR.7.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BMA_MAA.2.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BMA_MAR.1.1
RES	36	Absence de protection physique et logique (cloisonnement…)	RES_02	BMA_MAR.6.1
RES	38	Matériel d'utilisation complexe ou peu ergonomique	MAT_11	BSP_FOU.2.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BMA_MAA.2.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BMA_EMA.1.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BGC_PRE.4.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BPE_ZOS.2.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BPE_SEM.1.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BMA_MAR.7.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BMA_MAR.6.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BMA_MAR.1.1
RES	40	Absence de protection physique et logique (cloisonnement…)	RES_01	BMA_MAA.1.1

4.3.1 RES_INF : Médium et supports

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INF	5	Supports enterrés non repérés	PHY_03	CIS_PSI.1.2
RES_INF	5	Supports enterrés non repérés	PHY_03	CIS_PSI.1.1
RES_INF	14	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.1
RES_INF	14	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.2
RES_INF	15	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.1
RES_INF	15	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.2
RES_INF	16	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.1
RES_INF	16	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.2
RES_INF	17	Médium et supports susceptibles d'émettre des rayonnements parasites compromettants	PHY_05	BPE_SEM.3.1
RES_INF	19	Support ou équipement de communication physiquement accessible permettant la pose d'un matériel d'écoute	ORG_01	FCO_NRO.2.1
RES_INF	19	Médium et supports disposant des caractéristiques permettant l'écoute passive (ex:Ethernet, systèmes de communication sans fil)	RES_02	BDM_COC.1.1
RES_INF	19	Médium et supports disposant des caractéristiques permettant l'écoute passive (ex:Ethernet, systèmes de communication sans fil)	RES_02	BDM_COC.2.1
RES_INF	19	Médium et supports disposant des caractéristiques permettant l'écoute passive (ex:Ethernet, systèmes de communication sans fil)	RES_02	BDM_COC.5.1
RES_INF	19	Médium et supports disposant des caractéristiques permettant l'écoute passive (ex:Ethernet, systèmes de communication sans fil)	RES_02	FCS_COP.1.1
RES_INF	19	Médium et supports disposant des caractéristiques permettant l'écoute passive (ex:Ethernet, systèmes de communication sans fil)	RES_02	BPE_SEM.3.1
RES_INF	23	Présence d'un réseau de communication avec l'extérieur permettant l'échange d'information	RES_02	BGC_GER.1.1
RES_INF	24	Possibilité d'altérer une communication	RES_02	FCO_NRO.2.1
RES_INF	28	Mauvaises conditions d'utilisation	MAT_14	CGS_OML.1.1
RES_INF	28	Vieillissement du support	ORG_13	BPE_SEM.4.1
RES_INF	28	Mauvaise fiabilité des supports	MAT_15	BGC_PRS.2.1
RES_INF	29	Médium et supports intégrants des caractéristiques techniques spécifiques à sa localisation (ex. : paramètres de configuration ADSL différents entre la France et le Royaume Uni)	RES_04	BGC_PRS.2.1
RES_INF	29	Mauvaise fiabilité des supports	MAT_15	BGC_PRS.2.1
RES_INF	29	Défaut de maintenance	ORG_27	CGS_GMA.1.2
RES_INF	29	Possibilité d'incompatibilité entre les supports et d'autres composants	RES_04	BGC_PRS.2.1
RES_INF	29	Mauvaises conditions d'utilisation	MAT_14	CGS_OML.1.1
RES_INF	29	Vieillissement du support	ORG_13	BPE_SEM.4.1
RES_INF	29	Défaut de maintenance	ORG_27	CGS_GMA.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INF	29	Défaut de maintenance	ORG_27	CET_EIP.1.3
RES_INF	32	Défaut de maintenance	ORG_27	CGS_GMA.1.2
RES_INF	32	Absence de plan de câblage	PHY_11	CIS_CSI.1.1
RES_INF	32	Défaut de maintenance	ORG_27	CGS_GMA.2.1
RES_INF	32	Défaut de maintenance	ORG_27	CET_EIP.1.3
RES_INF	32	Absence de plan de câblage	PHY_11	CIS_ADL.3.1
RES_INF	32	La maintenance ou l'exploitation des équipements nécessite la disponibilité des supports réseau	RES_02	CAR_PAR.1.1
RES_INF	36	Possibilité d'agir sur les données transmises par l'intermédiaire du média de communication	RES_02	BDM_COC.2.1
RES_INF	37	Présence de point d'écoute illicite	RES_02	BDM_COC.2.1
RES_INF	37	Présence de point d'écoute illicite	RES_02	BDM_COC.1.1
RES_INF	37	Présence de point d'écoute illicite	RES_02	BPE_SEM.3.1
RES_INF	37	Présence de point d'écoute illicite	RES_02	BDM_COC.5.1
RES_INF	37	Présence de point d'écoute illicite	RES_02	FCS_COP.1.1
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.2
RES_INF	38	Absence d'étiquetage et de schéma d'architecture à jour	MAT_06	BCM_RLC.1.1
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.2
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.3
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.1
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.3
RES_INF	38	Absence de plan de câblage	PHY_11	CIS_ADL.3.1
RES_INF	38	Absence de plan de câblage	PHY_11	CIS_CSI.1.1
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.1
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.1
RES_INF	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.2
RES_INF	39	Absence de protection physique et logique	RES_01	BPE_SEM.1.1
RES_INF	39	Absence de protection physique et logique	RES_01	BPE_ZOS.2.1
RES_INF	39	Absence de protection physique et logique	RES_01	BMA_MAR.6.1
RES_INF	39	Absence de protection physique et logique	RES_01	BMA_EMA.1.1
RES_INF	39	Absence de protection physique et logique	RES_01	BMA_MAA.1.1
RES_INF	39	Absence de protection physique et logique	RES_01	BMA_MAR.7.1
RES_INF	39	Absence de protection physique et logique	RES_01	BMA_MAA.2.1
RES_INF	39	Absence de protection physique et logique	RES_01	BMA_MAR.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_01	BGC_PRE.4.1
RES_INF	40	Les interfaces sont connectées à des réseaux externes	RES_01	BPE_SEM.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_02	BGC_PRE.4.1
RES_INF	40	Les supports et médium sont connectés à des réseaux externes	RES_01	FTA_TAB.1.1
RES_INF	40	Les supports et médium sont connectés à des réseaux externes	RES_01	BPE_SEM.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_02	BMA_EMA.1.1
RES_INF	40	Possibilité de modifier des caractéristiques techniques (ex. : adresse MAC d'une carte Ethernet)	LOG_11	CGS_GDH.2.1
RES_INF	40	Les interfaces sont connectées à des réseaux externes	RES_01	FTA_TAB.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INF	40	Absence de cloisonnement réseau	RES_01	BMA_MAR.7.1
RES_INF	40	Absence de cloisonnement réseau	RES_01	BMA_MAR.6.1
RES_INF	40	Absence de cloisonnement réseau	RES_02	BMA_MAA.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_01	BMA_MAR.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_02	BMA_MAA.2.1
RES_INF	40	Absence de cloisonnement réseau	RES_01	BMA_MAA.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_01	BMA_EMA.1.1
RES_INF	40	Possibilité de modifier des caractéristiques techniques (ex. : adresse MAC d'une carte Ethernet)	LOG_11	CGS_GDH.1.2
RES_INF	40	Absence de protection physique	RES_01	CIS_PSI.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_02	BMA_MAR.1.1
RES_INF	40	Absence de cloisonnement réseau	RES_02	BMA_MAR.6.1
RES_INF	40	Absence de cloisonnement réseau	RES_02	BMA_MAR.7.1
RES_INF	40	Absence de cloisonnement réseau	RES_01	BMA_MAA.2.1
RES_INF	41	Absence de dispositif de traces et d'audit	RES_03	BDM_COC.4.1
RES_INF	41	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_INF	41	Les supports et médium sont accessibles à tous et actifs par défaut (ex. : ensemble des prises RJ45 brassées)	RES_01	BDM_COC.4.1
RES_INF	41	Les relais sont accessibles à tous	RES_01	BDM_COC.4.1
RES_INF	41	Le support permet d'utiliser les services du système depuis l'extérieur	RES_01	BDM_COC.4.1
RES_INF	41	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_INF	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)	MAT_12	BSP_FOU.2.1
RES_INF	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)	MAT_12	CEI_CDT.2.1
RES_INF	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)	MAT_12	CEI_CDT.2.2

4.3.2 RES_REL : Relais passif ou actif

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_REL	5	Fragilité des équipements	ORG_04	BSP_FOU.1.1
RES_REL	5	Equipement accessible à des personnes non autorisées	ORG_01	BPE_SEM.1.1
RES_REL	5	Equipement accessible à des personnes non autorisées	ORG_01	BPE_ZOS.1.1
RES_REL	5	Equipement accessible à des personnes non autorisées	ORG_01	BPE_ZOS.2.1
RES_REL	5	Equipement accessible à des personnes non autorisées	ORG_01	CET_EGT.2.3
RES_REL	5	Fragilité des équipements	ORG_04	BPE_SEM.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_REL	5	Fragilité des équipements	ORG_04	BPE_SEM.2.1
RES_REL	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)	PHY_01	BPE_SEM.4.1
RES_REL	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)	PHY_01	BPE_SEM.2.1
RES_REL	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)	PHY_01	CAR_AAR.1.1
RES_REL	13	Matériel maintenu à distance par des moyens de télécommunication	PHY_01	CAR_AAR.1.1
RES_REL	13	Matériel maintenu à distance par des moyens de télécommunication	PHY_01	BPE_SEM.4.1
RES_REL	13	Matériel maintenu à distance par des moyens de télécommunication	PHY_01	BPE_SEM.2.1
RES_REL	14	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.1
RES_REL	14	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.2
RES_REL	15	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.2
RES_REL	15	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.1
RES_REL	16	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.1
RES_REL	16	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques	PHY_10	CIS_PSI.1.2
RES_REL	17	Médium et supports susceptibles d'émettre des rayonnements parasites compromettants	PHY_05	BPE_SEM.3.1
RES_REL	17	Matériel susceptible d'émettre des rayonnements parasites compromettants	PHY_05	BPE_SEM.3.1
RES_REL	19	Communication s'effectuant en mode Broadcast	RES_02	BDM_COC.2.1
RES_REL	19	Accès physique ou logique à un relais permettant la pose d'un dispositif d'écoute	RES_01	BPE_ZOS.1.1
RES_REL	19	Accès physique ou logique à un relais permettant la pose d'un dispositif d'écoute	RES_01	BDM_COC.2.1
RES_REL	23	Absence de filtrage et de journalisation sur les relais de communication inter-reseau	RES_03	BMA_SAS.2.1
RES_REL	23	Absence de filtrage et de journalisation sur les relais de communication inter-reseau	RES_03	BMA_SAS.3.1
RES_REL	23	Absence de notification des utilisateurs	RES_03	BMA_MAS.6.1
RES_REL	23	Absence de notification des utilisateurs	RES_03	BGC_EIL.5.1
RES_REL	23	Absence de notification des utilisateurs	RES_03	BGC_EIL.4.1
RES_REL	23	Absence de filtrage et de journalisation sur les relais de communication inter-reseau	RES_03	BMA_SAS.1.1
RES_REL	23	Absence de filtrage et de journalisation sur les relais de communication inter-reseau	RES_02	CGS_CSR.1.2
RES_REL	24	Les relais n'identifient ni les sources ni les destinations (exemple d'impact : système vulnérable aux attaques basées sur "spoofing")	RES_03	FCO_NRO.2.1
RES_REL	24	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_REL	24	Possibilité d'utiliser les ressources sans trace	RES_03	FCO_NRO.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_REL	26	Possibilité d'utiliser les ressources sans trace	RES_03	BDM_COC.4.1
RES_REL	26	La liaison de télémaintenance est activée en permanence	RES_06	BMA_MAR.5.1
RES_REL	26	La couche SNMP est activée	RES_06	BDM_COC.4.1
RES_REL	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
RES_REL	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BMA_MAR.4.1
RES_REL	26	Possibilité d'utiliser les ressources sans trace	RES_03	FIA_UAU.1.2/2.1
RES_REL	26	Possibilité d'administrer le système à distance	RES_06	BGC_PLM.1.1
RES_REL	26	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
RES_REL	26	Possibilité d'utiliser les ressources sans trace	RES_03	BMA_MAR.4.1
RES_REL	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
RES_REL	26	Possibilité d'utiliser les ressources sans trace	RES_03	FCO_NRO.2.1
RES_REL	26	Possibilité d'utiliser les ressources sans trace	RES_03	FCO_NRO.2.1
RES_REL	26	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_REL	26	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_REL	26	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BDM_COC.4.1
RES_REL	26	Possibilité d'ajouter des dérivations logicielles	RES_01	BGC_PLM.1.1
RES_REL	26	Possibilité d'ajouter des logiciels additionnels pour stocker, transmettre ou altérer (ex. : keylogger)	RES_01	BGC_PLM.1.1
RES_REL	26	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BMA_MAA.1.1
RES_REL	26	Possibilité d'utiliser les ressources sans trace	RES_03	FCO_NRO.2.1
RES_REL	28	Mauvaise fiabilité des matériels	MAT_15	BGC_PRS.2.1
RES_REL	28	Vieillissement du matériel	ORG_13	BPE_SEM.4.1
RES_REL	29	Défaut de maintenance	ORG_27	CGS_GMA.1.2
RES_REL	29	Vieillissement du matériel	ORG_13	BPE_SEM.4.1
RES_REL	29	Mauvaise fiabilité des matériels	MAT_15	BGC_PRS.2.1
RES_REL	29	Défaut de maintenance	ORG_27	CET_EIP.1.3
RES_REL	29	Défaut de maintenance	ORG_27	CGS_GMA.2.1
RES_REL	29	Possibilité de mal configurer, installer ou de modifier les relais	RES_04	BMA_MAR.8.1
RES_REL	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)	LOG_14	FRU_FLT.1.1
RES_REL	30	Possibilité de mal configurer, installer ou de modifier les relais	RES_04	BMA_MAR.8.1
RES_REL	30	Mauvais dimensionnement (ex: trop de données par rapport à la bande passante maximale)	RES_02	BGC_PRS.1.1
RES_REL	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)	MAT_05	CAR_PAR.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_REL	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)	MAT_05	CAR_AAR.1.1
RES_REL	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)	MAT_05	FRU_FLT.1.1
RES_REL	31	Absence de procédure de maintenance	ORG_41	CDO_APP.1.2
RES_REL	31	Possibilité de mal configurer, installer ou de modifier les relais	RES_04	CGS_PPS.2.2
RES_REL	31	Absence de procédure de maintenance	ORG_41	CDO_APP.1.1
RES_REL	31	Absence de procédure de maintenance	ORG_41	BGC_PRE.1.1
RES_REL	32	Matériels spécifiques	ORG_09	BGC_PRS.2.1
RES_REL	32	Défaut de maintenance	ORG_27	CGS_GMA.2.1
RES_REL	32	Défaut de maintenance	ORG_27	CET_EIP.1.3
RES_REL	32	La maintenance ou l'exploitation du système se fait par l'intermédiaire du réseau	RES_02	CAR_PAR.1.1
RES_REL	32	Absence de garantie de supports des délais maximums	MAT_04	BGC_MSS.1.1
RES_REL	32	Défaut de maintenance	ORG_27	CGS_GMA.1.2
RES_REL	32	Matériels obsolètes	ORG_13	BPE_SEM.4.1
RES_REL	32	Matériels à configurations non évolutives	ORG_13	BPE_SEM.4.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	BGC_PRE.4.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_GAU.2.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAR.7.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAS.2.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAS.3.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	CGS_GDH.1.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	BCO_CEL.5.1
RES_REL	36	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BMA_MAA.1.1
RES_REL	36	La couche SNMP est activée	RES_06	BDM_COC.4.1
RES_REL	36	La liaison de télémaintenance est activée en permanence	RES_06	BDM_COC.4.1
RES_REL	36	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BMA_MAA.1.1
RES_REL	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
RES_REL	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
RES_REL	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1
RES_REL	36	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
RES_REL	36	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAA.1.1
RES_REL	37	Présence de point d'écoute illicite	RES_02	BDM_COC.2.1
RES_REL	37	Présence de point d'écoute illicite	RES_02	BDM_COC.5.1
RES_REL	37	Présence de point d'écoute illicite	RES_02	FCS_COP.1.1
RES_REL	37	Présence de point d'écoute illicite	RES_02	BPE_SEM.3.1
RES_REL	37	Présence de point d'écoute illicite	RES_02	BDM_COC.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.1
RES_REL	38	Médium et supports intégrants des caractéristiques techniques spécifiques à sa localisation (ex. : paramètres de configuration ADSL différents entre la France et le Royaume Uni)	RES_04	BGC_PRS.2.1
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.3
RES_REL	38	Absence d'étiquetage et de schéma d'architecture à jour	MAT_06	BCM_RLC.1.1
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.2
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.1
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.2
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.1
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.2
RES_REL	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.3
RES_REL	39	Le principe du moindre privilège n'est pas appliqué	LOG_11	CGS_GDH.2.1
RES_REL	39	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_REL	39	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_REL	39	Possibilité d'utiliser les ressources sans trace	RES_03	BDM_COC.4.1
RES_REL	39	Possibilité d'utiliser les ressources sans trace	RES_03	FCO_NRO.2.1
RES_REL	39	Possibilité d'utiliser les ressources sans trace	RES_03	FIA_UAU.1.2/2.1
RES_REL	39	Possibilité d'utiliser les ressources sans trace	RES_03	BMA_MAR.4.1
RES_REL	39	Le principe du moindre privilège n'est pas appliqué	LOG_11	CGS_GDH.1.2
RES_REL	40	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BMA_MAA.1.1
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	CGS_GDH.1.1
RES_REL	40	Absence de cloisonnement réseau	RES_02	BGC_PRE.4.1
RES_REL	40	Présence de protocole ne disposant pas de fonction d'authentification	RES_03	BDM_COC.4.1
RES_REL	40	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_REL	40	Absence de protection physique	ORG_01	CIS_PSI.1.1
RES_REL	40	Absence de protection physique	ORG_01	CIS_PSI.1.2
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAS.3.1
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAS.2.1
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAR.7.1
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_MAA.1.1
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	BMA_GAU.2.1
RES_REL	40	La liaison de télémaintenance est activée en permanence	RES_06	BMA_MAR.5.1
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	BCO_CEL.5.1
RES_REL	40	Absence de protection physique	RES_01	CIS_PSI.1.1
RES_REL	40	Absence de cloisonnement réseau	RES_02	BMA_MAR.7.1
RES_REL	40	Absence de cloisonnement réseau	RES_02	BMA_MAR.6.1
RES_REL	40	Absence de cloisonnement réseau	RES_02	BMA_MAR.1.1
RES_REL	40	Absence de cloisonnement réseau	RES_02	BMA_MAA.2.1
RES_REL	40	Absence de cloisonnement réseau	RES_02	BMA_MAA.1.1
RES_REL	40	Absence de cloisonnement réseau	RES_02	BMA_EMA.1.1
RES_REL	40	Possibilité d'administrer le système à distance	RES_06	BDM_COC.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_REL	40	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
RES_REL	40	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_REL	40	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BMA_MAA.1.1
RES_REL	40	Absence de dispositif de contrôle d'accès robuste	RES_01	BGC_PRE.4.1
RES_REL	40	Les relais n'identifient ni les sources ni les destinations (exemple d'impact : système vulnérable aux attaques basées sur "spoofing")	RES_03	FCO_NRO.2.1
RES_REL	41	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BDM_COC.4.1
RES_REL	41	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_REL	41	Absence de dispositif de traces et d'audit	RES_03	BDM_COC.4.1
RES_REL	41	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_REL	41	Les relais sont accessibles à tous	RES_01	BDM_COC.4.1
RES_REL	41	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BDM_COC.4.1
RES_REL	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)	MAT_12	BSP_FOU.2.1
RES_REL	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)	MAT_12	CEI_CDT.2.1
RES_REL	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)	MAT_12	CEI_CDT.2.2

4.3.3 RES_INT : Interface de communication

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INT	5	Fragilité des équipements	ORG_04	BSP_FOU.1.1
RES_INT	5	Fragilité des équipements	ORG_04	BPE_SEM.2.1
RES_INT	5	Fragilité des équipements	ORG_04	BPE_SEM.1.1
RES_INT	5	Equipement accessible à des personnes non autorisées	ORG_01	CET_EGT.1.1
RES_INT	5	Equipement accessible à des personnes non autorisées	ORG_01	BPE_ZOS.1.1
RES_INT	5	Equipement accessible à des personnes non autorisées	ORG_01	BPE_SEM.1.1
RES_INT	17	Matériel susceptible d'émettre des rayonnements parasites compromettants	PHY_05	BPE_SEM.3.1
RES_INT	19	Communication s'effectuant en mode Broadcast	RES_02	BDM_COC.2.1
RES_INT	19	Interface disposant d'une fonction permettant à l'écoute	RES_01	BMA_MAR.5.1
RES_INT	19	Complexité du routage entre les sous-réseaux	RES_05	BMA_MAR.8.1
RES_INT	19	Accès physique ou logique à un relais permettant la pose d'un dispositif d'écoute	PHY_03	BPE_ZOS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INT	19	Accès physique ou logique à un relais permettant la pose d'un dispositif d'écoute	RES_01	BDM_COC.2.1
RES_INT	19	Interface disposant d'une fonction permettant à l'écoute	RES_02	BMA_MAR.5.1
RES_INT	19	Absence d'authentification des matériels connectés au réseau	RES_03	BMA_MAS.1.1
RES_INT	23	Interface standard permettant les échanges de l'information (ex: interface Bluetooth acceptant toutes les communications par défaut)	RES_02	BDM_COC.1.1
RES_INT	23	Interface standard permettant les échanges de l'information (ex: interface Bluetooth acceptant toutes les communications par défaut)	RES_02	BDM_COC.2.1
RES_INT	23	Interface standard permettant les échanges de l'information (ex: interface Bluetooth acceptant toutes les communications par défaut)	RES_02	BDM_COC.5.1
RES_INT	23	Possibilité d'utiliser les ressources sans trace	RES_03	FCO_NRO.2.1
RES_INT	23	Interface standard permettant les échanges de l'information (ex: interface Bluetooth acceptant toutes les communications par défaut)	RES_02	FCS_COP.1.1
RES_INT	23	Absence de routage strict entre les sous-réseaux	RES_05	BPE_SEM.3.1
RES_INT	23	Complexité du routage entre les sous-réseaux	RES_05	BMA_MAR.8.1
RES_INT	23	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_INT	23	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_INT	23	Interface standard permettant les échanges de l'information (ex: interface Bluetooth acceptant toutes les communications par défaut)	RES_02	BPE_SEM.3.1
RES_INT	23	Absence de notification des utilisateurs	RES_03	FDP_UCT.1.1
RES_INT	24	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_INT	24	Possibilité d'utiliser les ressources sans trace	RES_03	FCO_NRO.2.1
RES_INT	24	Protocole ne permettant pas d'authentifier de manière sûre l'émetteur d'une communication	RES_03	FCO_NRO.2.1
RES_INT	26	Possibilité d'ajouter des logiciels additionnels pour stocker, transmettre ou altérer (ex. : keylogger)	RES_01	BGC_PLM.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.2
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.2.3
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.2
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FTA_TSE.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	CAR_PAR.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	BDM_COC.4.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_06	BGC_PLM.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	BGC_PLM.1.1
RES_INT	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INT	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.4.1
RES_INT	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
RES_INT	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
RES_INT	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BMA_MAR.4.1
RES_INT	26	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	FCO_NRO.1.1
RES_INT	26	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_INT	26	Possibilité d'ajouter des dérivations logicielles	RES_01	BGC_PLM.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FMT_MOF.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITA.1.1
RES_INT	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
RES_INT	26	Possibilité d'utiliser les ressources sans trace	RES_03	FIA_UAU.1.2/2.1
RES_INT	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
RES_INT	26	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BGC_PLM.1.1
RES_INT	26	La couche SNMP est activée	RES_06	BDM_COC.4.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.3.2
RES_INT	26	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BDM_COC.4.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.1.1
RES_INT	26	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BMA_MAA.1.1
RES_INT	26	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.2.1
RES_INT	26	La liaison de télémaintenance est activée en permanence	RES_06	BMA_MAR.5.1
RES_INT	28	Mauvaise fiabilité des matériels	MAT_15	BGC_PRS.2.1
RES_INT	28	Vieillissement du matériel	ORG_13	BPE_SEM.4.1
RES_INT	29	Mauvaise fiabilité des matériels	MAT_15	BGC_PRS.2.1
RES_INT	29	Possibilité de mal configurer, installer ou de modifier les relais	RES_04	BMA_MAR.8.1
RES_INT	29	Vieillissement du matériel	ORG_13	BPE_SEM.4.1
RES_INT	29	Possibilité d'incompatibilité entre les différentes ressources	RES_04	CIS_PSI.1.2
RES_INT	29	Interface intégrant des caractéristiques techniques relatives au pays (ex: prises téléphoniques différentes entre la France et le Royaume Uni)	RES_04	CIS_PSI.1.2
RES_INT	30	Possibilité de mal configurer, installer ou de modifier les relais	RES_04	BMA_MAR.8.1
RES_INT	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)	MAT_05	CAR_PAR.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INT	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)	LOG_14	CAR_AAR.1.1
RES_INT	31	Possibilité de mal configurer, installer ou de modifier les relais	RES_04	CGS_PPS.2.2
RES_INT	31	Mauvaise gestion des versions et configurations des pilotes	RES_04	CGS_PPS.2.3
RES_INT	31	Absence de procédure de maintenance	ORG_41	BGC_PRE.1.1
RES_INT	31	Absence de procédure de maintenance	ORG_41	CDO_APP.1.2
RES_INT	31	Effets de bord des interfaces (problèmes de compatibilité entre protocoles...)	RES_04	BGC_PRS.2.1
RES_INT	31	Absence de procédure de maintenance	ORG_41	CDO_APP.1.1
RES_INT	32	Matériels spécifiques	ORG_09	BGC_PRS.2.1
RES_INT	32	Absence de garantie de supports des délais maximums	MAT_04	BGC_MSS.1.1
RES_INT	32	La maintenance ou l'exploitation du système se fait par l'intermédiaire du réseau	RES_02	CAR_PAR.1.1
RES_INT	32	Matériels à configurations non évolutives	ORG_13	BGC_PRS.2.1
RES_INT	32	Matériels obsolètes	ORG_13	BPE_SEM.4.1
RES_INT	36	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BMA_MAA.1.1
RES_INT	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1
RES_INT	36	La couche SNMP est activée	RES_06	BDM_COC.4.1
RES_INT	36	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BMA_MAA.1.1
RES_INT	36	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
RES_INT	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
RES_INT	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
RES_INT	36	La liaison de télémaintenance est activée en permanence	RES_06	BDM_COC.4.1
RES_INT	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.2.1
RES_INT	38	Interface intégrant des caractéristiques techniques relatives au pays (ex: prises téléphoniques différentes entre la France et le Royaume Uni)	RES_04	BGC_PRS.2.1
RES_INT	39	Le principe du moindre privilège n'est pas appliqué	LOG_11	CGS_GDH.1.2
RES_INT	39	Le principe du moindre privilège n'est pas appliqué	LOG_11	CGS_GDH.2.1
RES_INT	39	Possibilité d'utiliser les ressources sans trace	RES_03	BMA_MAR.4.1
RES_INT	39	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1
RES_INT	40	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
RES_INT	40	Les interfaces sont accessibles à tous	RES_01	BMA_MAA.1.1
RES_INT	40	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BMA_MAA.1.1
RES_INT	40	Fichiers d'imputation complexes ou peu ergonomiques	ORG_42	BMA_GAU.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES_INT	40	La liaison de télémaintenance est activée en permanence	RES_06	BMA_MAR.5.1
RES_INT	40	Présence de protocole ne disposant pas de fonction d'authentification	RES_03	BDM_COC.4.1
RES_INT	40	Possibilité d'administrer le système à distance	RES_06	BDM_COC.4.1
RES_INT	40	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BMA_MAA.1.1
RES_INT	41	Le protocole ne permet pas l'identification sûr de l'émetteur	RES_03	FCO_NRO.1.1
RES_INT	41	Possibilité d'utiliser les ressources sans trace	RES_03	BDM_COC.4.1
RES_INT	41	Le réseau facilite l'utilisation des ressources par des personnes non autorisées	RES_01	BDM_COC.4.1
RES_INT	41	Le protocole ne permet pas l'envoi d'accusé de réception	RES_03	BDM_COC.4.1
RES_INT	41	Le réseau permet de modifier ou d'agir sur les ressources du système	RES_01	BDM_COC.4.1

4.4 PER : Personnel

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	1	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	1	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER	1	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	2	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	2	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER	2	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	3	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER	3	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	3	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	4	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	4	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	5	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	5	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	6	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	6	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	7	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	7	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	8	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	8	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	9	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.4
PER	9	Méconnaissance des mesures de sécurité	PER_11	CCS_SIN.3.5
PER	11	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.2
PER	11	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.7
PER	11	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.3
PER	11	Méconnaissance des mesures de sécurité	PER_11	BCA_AGC.5.1
PER	11	Méconnaissance des mesures de sécurité	PER_11	BCA_AGC.1.1
PER	11	Méconnaissance des mesures de sécurité	PER_11	BSP_FOU.1.1
PER	12	Méconnaissance des mesures de sécurité	PER_11	BCA_AGC.5.1
PER	12	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.3
PER	12	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.2
PER	12	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.7
PER	12	Méconnaissance des mesures de sécurité	PER_11	BSP_FOU.1.1
PER	12	Méconnaissance des mesures de sécurité	PER_11	BCA_AGC.1.1
PER	13	Méconnaissance des mesures de sécurité	PER_11	BCA_AGC.5.1
PER	13	Méconnaissance des mesures de sécurité	PER_11	BCA_AGC.1.1
PER	13	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.7
PER	13	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.2
PER	13	Méconnaissance des mesures de sécurité	PER_11	CCS_SSE.1.3
PER	13	Méconnaissance des mesures de sécurité	PER_11	BSP_FOU.1.1
PER	18	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	18	Faible sensibilisation à la protection de l'information	PER_02	BCO_CEL.4.1
PER	18	Faible sensibilisation à la protection de l'information	PER_02	BSP_FOU.1.1
PER	18	Méconnaissance des mesures de sécurité	PER_03	BGC_EIL.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	18	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	18	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER	18	Méconnaissance des mesures de sécurité	PER_03	BCM_CLI.1.1
PER	18	Méconnaissance des mesures de sécurité	PER_03	BGC_MSS.3.1
PER	18	Faible sensibilisation à la protection de l'information	PER_02	BCM_CLI.2.1
PER	18	Faible sensibilisation à la protection de l'information	PER_02	BCM_CLI.1.1
PER	18	Faible sensibilisation à la protection de l'information	PER_02	BPS_PSI.1.5
PER	19	Personnel manipulable	PER_02	CFO_SPS.1.1
PER	19	Faible sensibilisation à la protection en confidentialité des échanges d'information	PER_09	BSP_SPR.3.1
PER	19	Faible sensibilisation à la protection en confidentialité des échanges d'information	PER_09	CFO_SPS.1.1
PER	19	Manque de formation aux mesures et outils de protection des échanges externe et interne	PER_03	BSP_FOU.1.1
PER	19	Manque de formation aux mesures et outils de protection des échanges externe et interne	PER_03	BGC_EIL.2.1
PER	19	Manque de formation aux mesures et outils de protection des échanges externe et interne	PER_03	BGC_EIL.4.1
PER	19	Obtention d'un avantage à la captation d'information	PER_08	BSP_RIS.5.1
PER	19	Obtention d'un avantage à la captation d'information	PER_08	BSP_RIS.5.2
PER	19	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	19	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	19	Obtention d'un avantage à la captation d'information	PER_08	BSP_SPR.3.1
PER	20	Non-respect des règles associées à la classification des informations	PER_03	BSP_RIS.5.2
PER	20	Absence de sensibilisation à la protection des documents à caractère confidentiel provoquant un manque de vigilance	PER_02	BPS_PSI.1.5
PER	20	Non-respect des règles associées à la classification des informations	PER_03	BSP_SPR.1.1
PER	20	Non-respect des règles associées à la classification des informations	PER_03	BSP_RIS.5.1
PER	20	Non-respect des règles associées à la classification des informations	PER_03	BPS_PSI.1.4
PER	20	Absence de sensibilisation à la protection des documents à caractère confidentiel provoquant un manque de vigilance	PER_02	BCM_CLI.1.1
PER	20	Personnel manipulable	PER_02	CFO_SPS.1.1
PER	20	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_SPR.3.1
PER	20	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_RIS.5.2
PER	20	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_RIS.5.1
PER	20	Non-respect des règles associées à la classification des informations	PER_03	BSP_SPR.4.1
PER	20	Non-respect des règles associées à la classification des informations	PER_03	BPS_PSI.1.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	20	Absence de sensibilisation à la protection des documents à caractère confidentiel provoquant un manque de vigilance	PER_02	BCM_CLI.2.1
PER	20	Absence de sensibilisation à la protection des documents à caractère confidentiel provoquant un manque de vigilance	PER_02	BCO_CEL.4.1
PER	20	Absence de sensibilisation à la protection des documents à caractère confidentiel provoquant un manque de vigilance	PER_02	BSP_FOU.1.1
PER	21	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BPE_SEM.5.1
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables	PER_08	BSP_RIS.5.2
PER	21	Obtention d'un avantage à la revente d'un matériel	PER_08	BSP_RIS.5.1
PER	21	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BMA_IMT.1.1
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables	PER_01	BSP_FOU.1.1
PER	21	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables	PER_01	BPE_SEM.5.1
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables	PER_01	CCS_CSG.1.3
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables	PER_01	BMA_IMT.1.1
PER	21	Personnel manipulable	PER_02	CFO_SPS.1.1
PER	21	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BSP_FOU.1.1
PER	21	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BMA_IMT.2.1
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables	PER_01	BMA_IMT.2.1
PER	21	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables	PER_08	BSP_RIS.5.1
PER	21	Obtention d'un avantage à la revente d'un matériel	PER_08	BSP_RIS.5.2
PER	22	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_RIS.5.2
PER	22	Personnel manipulable	PER_02	CFO_SPS.1.1
PER	22	Non-respect des règles de destruction des supports associées à la classification de l'information	PER_02	BSP_RIS.5.1
PER	22	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_SPR.3.1
PER	22	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_RIS.5.1
PER	22	Non-respect des règles de destruction des supports associées à la classification de l'information	PER_02	BPE_MMG.2.1
PER	22	Non-respect des règles de destruction des supports associées à la classification de l'information	PER_02	BSP_FOU.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	22	Non-respect des règles de destruction des supports associées à la classification de l'information	PER_02	BPE_SEM.6.1
PER	22	Absence d'information et de sensibilisation à la rémanence des données informatiques sur les supports	PER_02	CFO_SPS.1.1
PER	22	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	22	Non-respect des règles de destruction des supports associées à la classification de l'information	PER_02	BGC_MSS.2.1
PER	22	Non-respect des règles de destruction des supports associées à la classification de l'information	PER_02	BSP_RIS.5.2
PER	22	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	23	Non-respect du devoir de réserve	PER_09	BSP_RIS.5.1
PER	23	Absence de sensibilisation à la protection de l'information à caractère sensible	PER_03	BSP_FOU.1.1
PER	23	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	23	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	23	Non-respect des règles de classification de l'information	PER_03	BSP_RIS.5.1
PER	23	Non-respect des règles de classification de l'information	PER_03	BSP_RIS.5.2
PER	23	Non-respect des règles de classification de l'information	PER_03	BPS_PSI.1.5
PER	23	Absence de sensibilisation à la protection de l'information à caractère sensible	PER_03	BPS_PSI.1.5
PER	23	Non-respect du devoir de réserve	PER_09	BSP_SPR.3.1
PER	23	Absence de sensibilisation à la protection de l'information à caractère sensible	PER_03	BCM_CLI.1.1
PER	23	Non-respect du devoir de réserve	PER_09	BSP_RIS.5.2
PER	23	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_RIS.5.1
PER	23	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_RIS.5.2
PER	23	Obtention d'un avantage à la divulgation d'information	PER_08	BSP_SPR.3.1
PER	23	Personnel manipulable	PER_02	CFO_SPS.1.1
PER	23	Non-respect des règles de classification de l'information	PER_03	BCM_CLI.1.1
PER	23	Absence de sensibilisation à la protection de l'information à caractère sensible	PER_03	BCM_CLI.2.1
PER	23	Absence de sensibilisation à la protection de l'information à caractère sensible	PER_03	BCO_CEL.4.1
PER	24	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	24	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	25	Absence de vigilance lors d'une intervention d'un personnel de maintenance sur un poste de travail ou un serveur	PER_05	BSP_FOU.1.1
PER	25	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BPE_SEM.5.1
PER	25	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BSP_FOU.1.1
PER	25	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BMA_IMT.2.1
PER	25	Faible sensibilisation à la protection des matériels en dehors de l'organisme	PER_01	BMA_IMT.1.1
PER	25	Absence de vigilance lors d'une intervention d'un personnel de maintenance sur un poste de travail ou un serveur	PER_05	CFO_SPS.1.1
PER	25	Absence de vigilance lors d'une intervention d'un personnel de maintenance sur un poste de travail ou un serveur	PER_05	CET_EIP.1.3
PER	25	Absence de vigilance lors d'une intervention d'un personnel de maintenance sur un poste de travail ou un serveur	PER_05	BOS_SAT.1.3
PER	25	Absence de vigilance lors d'une intervention d'un personnel de maintenance sur un poste de travail ou un serveur	PER_05	CET_EIP.1.5
PER	25	Absence de vigilance lors d'une intervention d'un personnel de maintenance sur un poste de travail ou un serveur	PER_05	CET_EIP.1.4
PER	25	Personnel manipulable	PER_02	CFO_SPS.1.1
PER	25	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.2
PER	25	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.1
PER	27	Méconnaissance des mesures de sécurité	PER_03	BGC_EIL.2.1
PER	27	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER	27	Méconnaissance des mesures de sécurité	PER_03	CPD_DGL.1.2
PER	27	Méconnaissance des mesures de sécurité	PER_03	CPD_DGL.1.1
PER	27	Manque de discrétion ou de vigilance	PER_09	CPD_DGL.1.2
PER	27	Méconnaissance des mesures de sécurité	PER_03	BPS_PSI.1.4
PER	27	Méconnaissance des mesures de sécurité	PER_03	BGC_MSS.3.1
PER	27	Méconnaissance des mesures de sécurité	PER_03	BCM_CLI.1.1
PER	27	Manque de discrétion ou de vigilance	PER_09	CPD_DGL.1.1
PER	27	Manque de discrétion ou de vigilance	PER_09	BSP_SPR.3.1
PER	27	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	27	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	33	Méconnaissance des mesures de sécurité	PER_03	CCS_CSG.1.1
PER	33	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER	34	Méconnaissance des mesures de sécurité	PER_03	BCO_CEL.2.1
PER	34	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER	34	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER	34	Méconnaissance des mesures de sécurité	PER_03	BCO_CEL.5.1
PER	34	Méconnaissance des mesures de sécurité	PER_03	BCO_CEL.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	34	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	34	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	34	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER	35	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER	35	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER	35	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1
PER	35	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER	35	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER	35	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER	35	Méconnaissance des mesures de sécurité	PER_03	BCO_CEL.5.1
PER	35	Méconnaissance des mesures de sécurité	PER_03	BCO_CEL.2.1
PER	35	Méconnaissance des mesures de sécurité	PER_03	BCO_CEL.1.1
PER	35	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	35	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	35	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER	36	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1
PER	36	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER	36	Absence de protection et de classification de l'information	ORG_15	BGC_MSS.3.1
PER	36	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	36	Absence de protection et de classification de l'information	ORG_15	BPS_PSI.1.5
PER	36	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	36	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER	36	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER	36	Absence de protection et de classification de l'information	ORG_15	BCM_CLI.2.1
PER	36	Personnel manipulable	PER_02	CFO_SPS.1.1
PER	36	Méconnaissance des mesures de sécurité	PER_03	CCS_CSG.1.1
PER	36	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER	36	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER	36	Absence de protection et de classification de l'information	ORG_15	BCM_CLI.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	36	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER	36	Absence de protection et de classification de l'information	ORG_15	BCM_CLI.1.2
PER	37	Absence de protection et de classification de l'information	ORG_15	BPS_PSI.1.5
PER	37	Absence de formation précisant les conditions d'utilisation licite de l'information	PER_10	BCO_CEL.5.1
PER	37	Absence de formation précisant les conditions d'utilisation licite de l'information	PER_10	BPS_PSI.1.3
PER	37	Absence de protection et de classification de l'information	ORG_15	BCM_CLI.1.1
PER	37	Absence de protection et de classification de l'information	ORG_15	BCM_CLI.1.2
PER	37	Absence de formation précisant les conditions d'utilisation licite de l'information	PER_10	BCO_CEL.4.1
PER	37	Absence de protection et de classification de l'information	ORG_15	BGC_MSS.3.1
PER	37	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER	37	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER	37	Méconnaissance des mesures de sécurité	PER_03	BCM_CLI.1.1
PER	37	Méconnaissance des mesures de sécurité	PER_03	BCM_CLI.1.2
PER	37	Méconnaissance des mesures de sécurité	PER_03	BCM_CLI.2.1
PER	37	Absence de protection et de classification de l'information	ORG_15	BCM_CLI.2.1
PER	37	Méconnaissance des mesures de sécurité	PER_03	BGC_MSS.3.1
PER	37	Absence de formation précisant les conditions d'utilisation licite de l'information	PER_10	BCO_CEL.1.1
PER	37	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER	37	Absence de formation précisant les conditions d'utilisation licite de l'information	PER_10	BCO_CEL.2.1
PER	39	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	39	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.1
PER	39	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.2
PER	39	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.3
PER	39	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.4
PER	39	La notion de droit n'est pas définie pour le personnel	PER_05	CGS_PAI.2.1
PER	39	La notion de droit n'est pas définie pour le personnel	PER_05	CGS_PAI.2.3
PER	39	La notion de droit n'est pas définie pour le personnel	PER_05	BSP_FOU.1.1
PER	39	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER	39	Obtention d'un avantage	PER_08	BSP_RIS.5.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER	39	Prééminence de la catégorie de personnel	PER_05	CGS_GDH.1.2
PER	39	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	40	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER	40	Organisation inadaptée	ORG_14	CGS_OES.1.1
PER	40	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER	40	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER	40	Missions peu adaptées au personnel	ORG_14	CRH_QDP.1.1
PER	40	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.4
PER	40	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.3
PER	40	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.2
PER	40	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.1
PER	40	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.7
PER	40	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.5
PER	40	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.4
PER	40	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.3
PER	40	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	40	Absence de règles morales ou d'éthique	PER_08	BSP_RIS.5.1
PER	40	Absence de règles morales ou d'éthique	PER_08	CCS_CHI.1.1
PER	40	Absence de règles morales ou d'éthique	PER_08	BSP_RIS.5.2
PER	40	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.1
PER	41	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER	41	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1

4.4.1 PER_DEC : Décisionnel

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEC	1	Absence de sensibilisation à la protection des équipements de sécurité	PER_05	CGS_HIS.1.1
PER_DEC	1	Absence de sensibilisation à la protection des équipements de sécurité	PER_05	CGS_HIS.1.2
PER_DEC	2	Absence de sensibilisation à la protection des équipements de sécurité	PER_05	CGS_HIS.1.1
PER_DEC	2	Absence de sensibilisation à la protection des équipements de sécurité	PER_05	CGS_HIS.1.2
PER_DEC	3	Absence de sensibilisation à la protection des équipements de sécurité	PER_05	CGS_HIS.1.1
PER_DEC	3	Absence de sensibilisation à la protection des équipements de sécurité	PER_05	CGS_HIS.1.2
PER_DEC	6	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEC	7	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_DEC	8	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_DEC	9	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_DEC	20	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BOS_ISI.1.1
PER_DEC	20	Absence de soutien de la direction à l'application de la politique de sécurité	PER_13	BPS_PSI.1.1
PER_DEC	24	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.1
PER_DEC	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCO_CEL.4.1
PER_DEC	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	BMA_REU.1.1
PER_DEC	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	BSP_FOU.1.1
PER_DEC	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CGS_GMP.1.1
PER_DEC	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CGS_GMP.1.3
PER_DEC	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CFO_SPS.1.1
PER_DEC	24	Crédulité	PER_02	CFO_SPS.1.1
PER_DEC	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BPS_PSI.1.5
PER_DEC	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BSP_FOU.1.1
PER_DEC	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCM_CLI.1.1
PER_DEC	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCO_CEL.1.1
PER_DEC	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	CFO_SPS.1.1
PER_DEC	24	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.2
PER_DEC	24	Personnel manipulable	PER_02	CFO_SPS.1.1
PER_DEC	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	BSP_FOU.1.1
PER_DEC	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.2
PER_DEC	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_RIS.5.2
PER_DEC	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BMA_GAU.2.1
PER_DEC	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BDM_SFS.1.1
PER_DEC	26	Utilisation de logiciels sans garantie de leur origine	PER_10	CGS_PPS.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEC	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	CGI_GIS.1.8
PER_DEC	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	BGC_PLM.1.1
PER_DEC	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BDM_SED.4.1
PER_DEC	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.1
PER_DEC	26	Personnel manipulable	PER_02	CFO_SPS.1.1
PER_DEC	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BSP_FOU.1.1
PER_DEC	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BSP_RIS.3.1
PER_DEC	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BGC_INT.3.1
PER_DEC	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BSP_RIS.1.1
PER_DEC	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	CFO_SPS.1.1
PER_DEC	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BGC_PLM.1.1
PER_DEC	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_FOU.1.1
PER_DEC	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_RIS.5.1
PER_DEC	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BMA_MAS.5.1
PER_DEC	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	CFO_SPS.1.1
PER_DEC	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.5
PER_DEC	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.4
PER_DEC	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	BGC_PRS.1.1
PER_DEC	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.3
PER_DEC	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.4
PER_DEC	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.3
PER_DEC	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.5
PER_DEC	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	BGC_PRS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEC	30	Absence de décision de redimensionnement à la vu d'augmentations significatives de l'utilisation des ressources informatiques	PER_05	BGC_PRS.1.1
PER_DEC	30	Absence de décision de redimensionnement à la vu d'augmentations significatives de l'utilisation des ressources informatiques	PER_05	CGI_GIS.3.6
PER_DEC	31	Absence de suivi des incidents permettant de prévenir d'éventuels dysfonctionnements (tableaux de bord)	PER_05	CGI_GIS.3.4
PER_DEC	31	Absence de suivi des incidents permettant de prévenir d'éventuels dysfonctionnements (tableaux de bord)	PER_05	CGI_GIS.3.2
PER_DEC	31	Absence de suivi des incidents permettant de prévenir d'éventuels dysfonctionnements (tableaux de bord)	PER_05	CGI_GIS.3.5
PER_DEC	31	Absence de suivi des incidents permettant de prévenir d'éventuels dysfonctionnements (tableaux de bord)	PER_05	CGI_GIS.3.1
PER_DEC	31	Absence de suivi des incidents permettant de prévenir d'éventuels dysfonctionnements (tableaux de bord)	PER_05	CGI_GIS.3.3
PER_DEC	32	Existence de composants désuets dans l'infrastructure de traitement de l'information (développement dans des langages plus utilisés…)	ORG_13	CEI_CDT.1.2
PER_DEC	32	Faible budget alloué à la maintenance	PER_13	CGS_GMA.5.1
PER_DEC	32	Existence de composants désuets dans l'infrastructure de traitement de l'information (développement dans des langages plus utilisés…)	ORG_13	CEI_CDT.1.1
PER_DEC	32	Choix de technologie sans assurance de pérennité	ORG_13	CEI_CDT.1.1
PER_DEC	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER_DEC	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER_DEC	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1
PER_DEC	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_DEC	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER_DEC	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.7
PER_DEC	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.4
PER_DEC	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.1
PER_DEC	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER_DEC	33	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER_DEC	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.3
PER_DEC	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.5
PER_DEC	33	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER_DEC	34	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEC	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_DEC	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER_DEC	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1
PER_DEC	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER_DEC	34	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER_DEC	38	Non-respect des consignes	PER_10	BSP_RIS.5.1
PER_DEC	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.1
PER_DEC	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.2
PER_DEC	38	Mauvaise connaissance des responsabilités	PER_05	BOS_ISI.3.1
PER_DEC	38	Mauvaise connaissance des responsabilités	PER_05	BPS_PSI.1.3
PER_DEC	38	Mauvaise connaissance des responsabilités	PER_05	BSP_SPR.1.1
PER_DEC	38	Mauvaise connaissance des responsabilités	PER_05	BSP_FOU.1.1
PER_DEC	38	Non-respect des consignes	PER_10	BCO_RPS.1.1
PER_DEC	38	Non-respect des consignes	PER_10	BCO_RPS.1.2
PER_DEC	38	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.4
PER_DEC	38	Non-respect des consignes	PER_10	BPS_PSI.1.4
PER_DEC	38	Mauvaise connaissance des responsabilités	PER_05	BSP_SPR.4.1
PER_DEC	38	Non-respect des consignes	PER_10	BSP_RIS.5.2
PER_DEC	38	Non-respect des consignes	PER_10	BSP_SPR.1.1
PER_DEC	38	Non-respect des consignes	PER_10	BSP_SPR.4.1
PER_DEC	38	Personnel utilisateur peu ou mal formé	PER_12	BSP_FOU.2.1
PER_DEC	38	Non-respect des consignes	PER_10	BCO_RPS.2.1
PER_DEC	38	Absence de formalisation des responsabilités connues de tous	PER_05	BOS_ISI.3.1
PER_DEC	38	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.3
PER_DEC	38	Absence de formalisation des responsabilités connues de tous	PER_05	BPS_PSI.1.3
PER_DEC	38	Absence de formalisation des responsabilités connues de tous	PER_05	BSP_SPR.1.1
PER_DEC	38	Absence de formalisation des responsabilités connues de tous	PER_05	BSP_SPR.4.1
PER_DEC	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.1
PER_DEC	38	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.2
PER_DEC	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.2
PER_DEC	38	Il existe des opérations très sensibles opérables par une personne unique	PER_07	CGS_GPC.2.1
PER_DEC	41	Changement de politique ou de stratégie d'organisation	ORG_14	CGS_OES.1.2
PER_DEC	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.4.1
PER_DEC	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.1.1
PER_DEC	41	Responsabilité de chacun non connue	PER_05	BPS_PSI.1.3
PER_DEC	41	Responsabilité de chacun non connue	PER_05	BOS_ISI.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEC	41	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER_DEC	41	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER_DEC	41	Changement de politique ou de stratégie d'organisation	ORG_14	BMA_MAS.3.1
PER_DEC	41	Changement de politique ou de stratégie d'organisation	ORG_14	CGS_OES.1.3
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	CRH_DDE.1.2
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	BSP_RIS.5.1
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	CRH_DDE.1.1
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	CFO_FRS.1.5
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	BSP_RIS.5.2
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	CFO_FRS.1.4
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	CFO_FRS.1.3
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	CFO_FRS.1.2
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel	PER_05	CFO_FRS.1.1

4.4.2 PER_UTI : Utilisateurs

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CRR_SEN.1.2
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.1.4
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.1
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.3
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CCS_SIN.2.3
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CCS_SIN.2.2
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CCS_SIN.2.1
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.6
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.5
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.4
PER_UTI	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.2
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CRR_SEN.1.1
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BSP_FOU.1.1
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BMA_IMT.1.1
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BMA_IMT.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_03	BSP_FOU.1.1
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CFO_SPS.1.1
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.2
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.4
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.3
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BPE_SEM.5.1
PER_UTI	6	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_UTI	7	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_UTI	8	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_UTI	9	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_UTI	12	Manque d'information concernant les conditions d'utilisation des points d'énergie secourue	PER_11	CCS_SSE.1.2
PER_UTI	12	Manque d'information concernant les conditions d'utilisation des points d'énergie secourue	PER_11	CCS_SSE.1.3
PER_UTI	12	Manque d'information concernant les conditions d'utilisation des points d'énergie secourue	PER_11	CCS_SSE.1.7
PER_UTI	12	Manque d'information concernant les conditions d'utilisation des points d'énergie secourue	PER_11	BSP_FOU.1.1
PER_UTI	12	Manque d'information concernant les conditions d'utilisation des points d'énergie secourue	PER_11	BCA_AGC.1.1
PER_UTI	12	Manque d'information concernant les conditions d'utilisation des points d'énergie secourue	PER_11	BCA_AGC.5.1
PER_UTI	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel	PER_05	BSP_SPR.3.1
PER_UTI	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel	PER_05	BSP_SPR.1.1
PER_UTI	24	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.1
PER_UTI	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	BSP_FOU.1.1
PER_UTI	24	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.2
PER_UTI	24	Personnel manipulable	PER_02	CFO_SPS.1.1
PER_UTI	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	CFO_SPS.1.1
PER_UTI	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	BMA_REU.1.1
PER_UTI	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCO_CEL.1.1
PER_UTI	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCM_CLI.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_UTI	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BSP_FOU.1.1
PER_UTI	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BPS_PSI.1.5
PER_UTI	24	Crédulité	PER_02	CFO_SPS.1.1
PER_UTI	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CFO_SPS.1.1
PER_UTI	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CGS_GMP.1.3
PER_UTI	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CGS_GMP.1.1
PER_UTI	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCO_CEL.4.1
PER_UTI	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BMA_GAU.2.1
PER_UTI	26	Personnel manipulable	PER_02	CFO_SPS.1.1
PER_UTI	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	BGC_PLM.1.1
PER_UTI	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	CFO_SPS.1.1
PER_UTI	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BDM_SED.4.1
PER_UTI	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.2
PER_UTI	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BMA_MAS.5.1
PER_UTI	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_FOU.1.1
PER_UTI	26	Utilisation de logiciels sans garantie de leur origine	PER_10	CGS_PPS.2.1
PER_UTI	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.1
PER_UTI	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	BSP_FOU.1.1
PER_UTI	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_RIS.5.2
PER_UTI	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BDM_SFS.1.1
PER_UTI	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	CFO_SPS.1.1
PER_UTI	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BGC_PLM.1.1
PER_UTI	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	CGI_GIS.1.8
PER_UTI	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BSP_RIS.3.1
PER_UTI	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BSP_RIS.1.1
PER_UTI	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BGC_INT.3.1
PER_UTI	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie	PER_11	BSP_FOU.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_UTI	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_RIS.5.1
PER_UTI	28	Méconnaissance des consignes d'usage des matériels	PER_03	BSP_FOU.1.1
PER_UTI	28	Absence de remontée d'information pour une analyse centralisée des pannes	PER_05	CGI_GIS.3.3
PER_UTI	28	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.1
PER_UTI	28	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.2
PER_UTI	28	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.3
PER_UTI	28	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.4
PER_UTI	28	Absence de remontée d'information pour une analyse centralisée des pannes	PER_05	CGI_GIS.3.1
PER_UTI	28	Absence de remontée d'information pour une analyse centralisée des pannes	PER_05	CGI_GIS.3.2
PER_UTI	29	Absence de remontée d'information pour une analyse centralisée des pannes	PER_05	CGI_GIS.3.2
PER_UTI	29	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.4
PER_UTI	29	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.3
PER_UTI	29	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.2
PER_UTI	29	Méconnaissance des consignes d'usage des matériels	PER_03	CCS_CSG.1.1
PER_UTI	29	Absence de remontée d'information pour une analyse centralisée des pannes	PER_05	CGI_GIS.3.3
PER_UTI	29	Absence de remontée d'information pour une analyse centralisée des pannes	PER_05	CGI_GIS.3.1
PER_UTI	29	Méconnaissance des consignes d'usage des matériels	PER_03	BSP_FOU.1.1
PER_UTI	30	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.1
PER_UTI	30	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.2
PER_UTI	30	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_03	BSP_FOU.2.1
PER_UTI	30	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_03	CCS_CSG.1.2
PER_UTI	30	Manque de sensibilisation aux besoins d'économie des ressources informatiques de l'organisme (mauvaise utilisation des espaces de stockage…)	PER_03	CCS_CSG.1.2
PER_UTI	31	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	BSP_FOU.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_UTI	31	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	CCS_CSG.1.2
PER_UTI	32	Non-respect des règles qualité	PER_10	BSP_RIS.5.2
PER_UTI	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	CGS_PPS.2.1
PER_UTI	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	BMA_MAS.5.1
PER_UTI	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	BMA_GAU.2.1
PER_UTI	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	BDM_SFS.1.1
PER_UTI	32	Non-respect des règles qualité	PER_10	BSP_FOU.1.1
PER_UTI	32	Non-respect des règles qualité	PER_10	BSP_RIS.5.1
PER_UTI	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.6
PER_UTI	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.3
PER_UTI	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.2
PER_UTI	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.1
PER_UTI	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	BSP_FOU.2.1
PER_UTI	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	CCS_CSG.1.2
PER_UTI	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	BSP_FOU.2.1
PER_UTI	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	CCS_CSG.1.2
PER_UTI	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	BDM_SED.4.1
PER_UTI	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.4
PER_UTI	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER_UTI	33	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER_UTI	33	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER_UTI	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_UTI	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER_UTI	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1
PER_UTI	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER_UTI	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.3
PER_UTI	33	Droits accordés en dehors du besoin légitime	PER_07	CGS_GDH.1.1
PER_UTI	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER_UTI	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_UTI	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER_UTI	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_UTI	34	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER_UTI	34	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER_UTI	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER_UTI	38	Non-respect des consignes	PER_10	BPS_PSI.1.4
PER_UTI	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.1
PER_UTI	38	Personnel utilisateur peu ou mal formé	PER_12	BSP_FOU.2.1
PER_UTI	38	Personnel peu habitué à la saisie	PER_06	CPS_PAQ.3.1
PER_UTI	38	Personnel peu habitué à la saisie	PER_06	BSP_FOU.2.1
PER_UTI	38	Non-respect des consignes	PER_10	BSP_SPR.4.1
PER_UTI	38	Non-respect des consignes	PER_10	BSP_SPR.1.1
PER_UTI	38	Non-respect des consignes	PER_10	BSP_RIS.5.2
PER_UTI	38	Non-respect des consignes	PER_10	BSP_RIS.5.1
PER_UTI	38	Absence de motivation pour les travaux associés à la saisie	PER_05	CPS_PAQ.2.1
PER_UTI	38	Non-respect des consignes	PER_10	BCO_RPS.1.1
PER_UTI	38	Absence de documentation d'utilisation des applicatifs existantes	PER_12	CDO_APP.1.1
PER_UTI	38	Non-respect des consignes	PER_10	BCO_RPS.2.1
PER_UTI	38	Absence de motivation pour les travaux associés à la saisie	PER_05	CPS_PAQ.2.2
PER_UTI	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.1
PER_UTI	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.2
PER_UTI	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.2
PER_UTI	38	Non-respect des consignes	PER_10	BCO_RPS.1.2
PER_UTI	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.1.1
PER_UTI	41	Responsabilité de chacun non connue	PER_05	BPS_PSI.1.3
PER_UTI	41	Responsabilité de chacun non connue	PER_05	BOS_ISI.3.1
PER_UTI	41	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER_UTI	41	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER_UTI	41	Changement de politique ou de stratégie d'organisation	ORG_14	BMA_MAS.3.1
PER_UTI	41	Changement de politique ou de stratégie d'organisation	ORG_14	CGS_OES.1.3
PER_UTI	41	Changement de politique ou de stratégie d'organisation	ORG_14	CGS_OES.1.2
PER_UTI	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.4.1
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_DDE.1.1
PER_UTI	42	Indisponibilité causée par la maladie	PER_04	CRH_DDE.1.2
PER_UTI	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.1
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	BSP_RIS.5.2
PER_UTI	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.2
PER_UTI	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_UTI	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.4
PER_UTI	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.5
PER_UTI	42	Indisponibilité causée par la maladie	PER_04	CRH_DDE.1.1
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_PDP.1.1
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.1
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.2
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.3
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_DDE.1.2
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.5
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	BSP_RIS.5.1
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.4
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.4
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.3
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	CRH_DDE.1.1
PER_UTI	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.1
PER_UTI	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.2
PER_UTI	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.3
PER_UTI	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.4
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	BSP_RIS.5.2
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	CRH_DDE.1.2
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.2
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.5
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	CFO_FRS.1.3
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	CRH_DDE.1.1
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.1
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	CFO_FRS.1.4
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	CFO_FRS.1.2
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	CFO_FRS.1.1
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	BSP_RIS.5.1
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_04	CRH_DDE.1.2
PER_UTI	42	Indisponibilité causée par l'absentéisme	PER_05	CFO_FRS.1.5

4.4.3 PER_EXP : Exploitant / Maintenance

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.1.4

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CCS_SIN.2.1
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.4
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.5
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.1
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.2
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.3
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CGI_GDC.3.6
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CCS_SIN.2.2
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CCS_SIN.2.3
PER_EXP	4	Absence de procédures de gestion de situation d'urgence	PER_11	CRR_SEN.1.2
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CRR_SEN.1.1
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BPE_SEM.5.1
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BSP_FOU.1.1
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BMA_IMT.1.1
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.2
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BMA_IMT.2.1
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_03	BSP_FOU.1.1
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CFO_SPS.1.1
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.4
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.3
PER_EXP	6	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_EXP	7	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_EXP	8	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_EXP	9	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_EXP	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel	PER_05	BSP_SPR.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_EXP	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel	PER_05	BSP_SPR.1.1
PER_EXP	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CGS_GMP.1.1
PER_EXP	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	BSP_FOU.1.1
PER_EXP	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	BMA_REU.1.1
PER_EXP	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BSP_FOU.1.1
PER_EXP	24	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.1
PER_EXP	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	CFO_SPS.1.1
PER_EXP	24	Personnel manipulable	PER_02	CFO_SPS.1.1
PER_EXP	24	Crédulité	PER_02	CFO_SPS.1.1
PER_EXP	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BPS_PSI.1.5
PER_EXP	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CGS_GMP.1.3
PER_EXP	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)	PER_03	CFO_SPS.1.1
PER_EXP	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCO_CEL.4.1
PER_EXP	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCM_CLI.1.1
PER_EXP	24	Méconnaissance de l'importance de la qualification de l'information	PER_10	BCO_CEL.1.1
PER_EXP	24	Obtention d'un avantage à la désinformation	PER_08	BSP_RIS.5.2
PER_EXP	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BGC_PLM.1.1
PER_EXP	26	Utilisation de logiciels sans garantie de leur origine	PER_10	CGS_PPS.2.3
PER_EXP	26	Utilisation de logiciels sans garantie de leur origine	PER_10	CGS_PPS.2.1
PER_EXP	26	Utilisation de logiciels sans garantie de leur origine	PER_10	CGS_OML.1.2
PER_EXP	26	Personnel manipulable	PER_02	CFO_SPS.1.1
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie	PER_03	BGC_PRE.1.1
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie	PER_03	CGI_GIS.1.1
PER_EXP	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.1
PER_EXP	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.2
PER_EXP	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	BSP_FOU.1.1
PER_EXP	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BDM_SFS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_EXP	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	CFO_SPS.1.1
PER_EXP	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BMA_MAS.5.1
PER_EXP	26	Exploitant ou mainteneur disposant de privilèges étendus	PER_02	BSP_RIS.5.2
PER_EXP	26	Exploitant ou mainteneur disposant de privilèges étendus	PER_02	BSP_RIS.5.1
PER_EXP	26	Exploitant ou mainteneur disposant de privilèges étendus	PER_02	BSP_SPR.1.1
PER_EXP	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_RIS.5.2
PER_EXP	26	Utilisation de logiciels sans garantie de leur origine	PER_10	BDM_SED.4.1
PER_EXP	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_FOU.1.1
PER_EXP	26	Manque de sensibilisation à la menace des codes malveillants	PER_03	BGC_PLM.1.1
PER_EXP	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	BSP_RIS.5.1
PER_EXP	26	Non-respect des règles de mises à jour des logiciels anti-virus	PER_03	CFO_SPS.1.1
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie	PER_03	BSP_FOU.1.1
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie	PER_03	CGI_GIS.1.8
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie	PER_03	BSP_RIS.3.1
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie	PER_03	BSP_RIS.1.1
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie	PER_03	BGC_INT.3.1
PER_EXP	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.3
PER_EXP	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.2
PER_EXP	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.1
PER_EXP	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.2
PER_EXP	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.3
PER_EXP	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.1
PER_EXP	30	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_EXP	30	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.2
PER_EXP	30	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.3
PER_EXP	30	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.4
PER_EXP	30	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	CGI_GIS.3.1
PER_EXP	30	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)	PER_05	BGC_PRS.1.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BSP_RIS.3.1
PER_EXP	31	Manque de formation à la maintenance et l'exploitation de nouveaux équipements	PER_12	BSP_FOU.2.1
PER_EXP	31	Mauvais dimensionnement des ressources d'exploitation ou de maintenance	ORG_09	CFO_FRS.2.2
PER_EXP	31	Mauvais dimensionnement des ressources d'exploitation ou de maintenance	ORG_09	CRH_DDE.1.1
PER_EXP	31	Mauvais dimensionnement des ressources d'exploitation ou de maintenance	ORG_09	CRH_DDE.1.2
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	CGI_GIS.1.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	CGI_GIS.1.8
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BGC_INT.3.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BGC_PRE.2.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BSP_RIS.1.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BDM_SED.1.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BDM_SED.3.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BGC_PRE.2.2
PER_EXP	31	Mauvais dimensionnement des ressources d'exploitation ou de maintenance	ORG_09	CEI_ABS.1.5
PER_EXP	31	Manque de formation à la maintenance et l'exploitation de nouveaux équipements	PER_12	CGS_GMA.2.1
PER_EXP	31	Non-respect des procédures d'intervention	PER_03	BSP_FOU.1.1
PER_EXP	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.6
PER_EXP	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	CCS_CSG.1.2
PER_EXP	32	Non-respect des règles qualité	PER_10	BSP_RIS.5.2
PER_EXP	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	CCS_CSG.1.2
PER_EXP	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	BSP_FOU.2.1
PER_EXP	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)	PER_12	BSP_FOU.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_EXP	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.1
PER_EXP	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.2
PER_EXP	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.3
PER_EXP	32	Non-respect des règles qualité	PER_10	BSP_RIS.5.1
PER_EXP	32	Non-respect des règles qualité	PER_10	BSP_FOU.1.1
PER_EXP	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	CGS_PPS.2.1
PER_EXP	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	CGS_PPS.2.3
PER_EXP	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	BMA_MAS.5.1
PER_EXP	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	BDM_SED.4.1
PER_EXP	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme	PER_10	BDM_SFS.1.1
PER_EXP	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER_EXP	33	Absence de gestion de parc du matériel	PER_05	CDO_SDC.1.1
PER_EXP	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER_EXP	33	Absence de charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_EXP	33	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER_EXP	33	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER_EXP	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_EXP	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER_EXP	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1
PER_EXP	34	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER_EXP	34	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER_EXP	34	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER_EXP	38	Personnel peu habitué à la saisie	PER_06	CPS_PAQ.3.1
PER_EXP	38	Absence de motivation pour les travaux associés à la saisie	PER_05	CPS_PAQ.2.1
PER_EXP	38	Absence de motivation pour les travaux associés à la saisie	PER_05	CPS_PAQ.2.2
PER_EXP	38	Non-respect des consignes	PER_10	BCO_RPS.1.2
PER_EXP	38	Non-respect des consignes	PER_10	BCO_RPS.1.1
PER_EXP	38	Personnel utilisateur peu ou mal formé	PER_12	BSP_FOU.2.1
PER_EXP	38	Absence de documentation d'utilisation des applicatifs existantes	PER_12	CDO_APP.1.1
PER_EXP	38	Personnel peu habitué à la saisie	PER_06	BSP_FOU.2.1
PER_EXP	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.2
PER_EXP	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.1
PER_EXP	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_EXP	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.1
PER_EXP	38	Non-respect des consignes	PER_10	BSP_SPR.1.1
PER_EXP	38	Non-respect des consignes	PER_10	BSP_RIS.5.2
PER_EXP	38	Non-respect des consignes	PER_10	BCO_RPS.2.1
PER_EXP	38	Non-respect des consignes	PER_10	BSP_RIS.5.1
PER_EXP	38	Non-respect des consignes	PER_10	BSP_SPR.4.1
PER_EXP	38	Non-respect des consignes	PER_10	BPS_PSI.1.4
PER_EXP	41	Responsabilité de chacun non connue	PER_05	BOS_ISI.3.1
PER_EXP	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.4.1
PER_EXP	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.1.1
PER_EXP	41	Responsabilité de chacun non connue	PER_05	BPS_PSI.1.3
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	CRH_DDE.1.1
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	CRH_DDE.1.2
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.5
PER_EXP	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.1
PER_EXP	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.4
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	BSP_RIS.5.1
PER_EXP	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.3
PER_EXP	42	Indisponibilité causée par la maladie	PER_04	CRH_DDE.1.1
PER_EXP	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.5
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.1
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.2
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.3
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	BSP_RIS.5.2
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_PDP.1.1
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.4
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_DDE.1.1
PER_EXP	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.2
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.1
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.2
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.3
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.4
PER_EXP	42	Indisponibilité causée par l'absentéisme	PER_04	CFO_FRS.1.5
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_DDE.1.2
PER_EXP	42	Indisponibilité causée par la maladie	PER_04	CRH_DDE.1.2

4.4.4 PER_DEV : Développeur

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.3
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_03	BSP_FOU.1.1
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BMA_IMT.2.1
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.2
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BMA_IMT.1.1
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BSP_FOU.1.1
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_01	BPE_SEM.5.1
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CCS_CSG.1.4
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CRR_SEN.1.1
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements	PER_03	CFO_SPS.1.1
PER_DEV	6	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_DEV	7	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_DEV	8	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_DEV	9	Absence de test des procédures de réaction et d'information en cas de sinistre	PER_11	CCS_SIN.3.5
PER_DEV	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel	PER_05	BSP_SPR.1.1
PER_DEV	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel	PER_05	BSP_SPR.3.1
PER_DEV	24	Méconnaissance des mesures de sécurité	PER_11	BPS_PSI.1.4
PER_DEV	24	Méconnaissance des mesures de sécurité	PER_11	BSP_FOU.1.1
PER_DEV	24	Absence de moyens permettant de garantir l'authenticité des codes	ORG_20	CGS_OML.1.3
PER_DEV	26	Personnel manipulable	PER_02	CFO_SPS.1.1
PER_DEV	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.2
PER_DEV	26	Obtention d'un avantage à la perturbation du système informatique	PER_08	BSP_RIS.5.1
PER_DEV	26	Méconnaissance des mesures de sécurité	PER_03	BPS_PSI.1.4
PER_DEV	26	Méconnaissance des mesures de sécurité	PER_03	BSP_FOU.1.1
PER_DEV	26	Absence de moyens permettant de garantir l'authenticité des développements	ORG_20	CGS_OML.1.3
PER_DEV	31	Absence de règles de sécurité dans les développements	PER_10	BDM_SED.4.1
PER_DEV	31	Absence de règles de sécurité dans les développements	PER_10	CPS_DEV.1.1
PER_DEV	31	Manque de formation	PER_12	BSP_FOU.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEV	31	Absence de règles de sécurité dans les développements	PER_10	BDM_SFS.3.1
PER_DEV	31	Absence de règles de sécurité dans les développements	PER_10	CPS_DEV.1.2
PER_DEV	32	Non-respect des règles de développement	PER_10	BSP_RIS.5.1
PER_DEV	32	Absence de standard ou de norme	PER_10	CPS_DEV.1.2
PER_DEV	32	Absence de standard ou de norme	PER_10	BDM_SED.4.1
PER_DEV	32	Absence de standard ou de norme	PER_10	BDM_SFS.3.1
PER_DEV	32	Non-respect des règles de développement	PER_10	CPS_DEV.1.1
PER_DEV	32	Non-respect des règles de développement	PER_10	CPS_DEV.1.2
PER_DEV	32	Non-respect des règles de développement	PER_10	BDM_SED.4.1
PER_DEV	32	Absence de standard ou de norme	PER_10	CPS_DEV.1.1
PER_DEV	32	Non-respect des règles de développement	PER_10	BSP_FOU.1.1
PER_DEV	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.2
PER_DEV	32	Non-respect des règles de développement	PER_10	BSP_RIS.5.2
PER_DEV	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.1
PER_DEV	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.3
PER_DEV	32	Non-respect des règles qualité	PER_10	BSP_RIS.5.1
PER_DEV	32	Non-respect des règles qualité	PER_10	BSP_RIS.5.2
PER_DEV	32	Non-respect des règles qualité	PER_10	BSP_FOU.1.1
PER_DEV	32	Non-respect des règles de développement	PER_10	BDM_SFS.3.1
PER_DEV	32	Non-respect des règles qualité	PER_10	CPS_PAQ.1.6
PER_DEV	33	Absence de règles morales ou d'éthique	PER_08	BSP_RIS.5.2
PER_DEV	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.2
PER_DEV	33	Absence de charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_DEV	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_FOU.1.1
PER_DEV	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	CCS_CHI.1.1
PER_DEV	33	Absence de règles morales ou d'éthique	PER_08	BSP_RIS.5.1
PER_DEV	33	Obtention d'un avantage	PER_08	BSP_RIS.5.1
PER_DEV	33	Absence de règles morales ou d'éthique	PER_08	CCS_CHI.1.1
PER_DEV	33	Obtention d'un avantage	PER_08	BSP_RIS.5.2
PER_DEV	33	Non-respect de la charte informatique précisant les exigences d'utilisation	PER_03	BSP_RIS.5.1
PER_DEV	33	Manque de contrôle des besoins matériels pour développer une application	ORG_32	CEI_ABS.1.5
PER_DEV	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.1
PER_DEV	33	Absence de sensibilisation du personnel au risque de sanction	PER_08	BSP_RIS.5.2
PER_DEV	35	Aucune procédure d'évaluation des produits	ORG_20	CGS_OML.1.1
PER_DEV	35	Aucune procédure d'évaluation des produits	ORG_20	CGS_PPS.2.3
PER_DEV	35	Absence de procédure et moyens de vérification de l'origine du logiciel (signature du code, du binaire…)	ORG_20	CGS_OML.1.1
PER_DEV	35	Aucune certification des produits	LOG_06	CGS_OML.1.2
PER_DEV	38	Non-respect des consignes	PER_10	BPS_PSI.1.4
PER_DEV	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PER_DEV	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.1
PER_DEV	38	Absence de motivation pour les travaux associés à la saisie	PER_05	CPS_PAQ.2.2
PER_DEV	38	Absence de motivation pour les travaux associés à la saisie	PER_05	CPS_PAQ.2.1
PER_DEV	38	Non-respect des consignes	PER_10	BCO_RPS.1.1
PER_DEV	38	Non-respect des consignes	PER_10	BCO_RPS.1.2
PER_DEV	38	Non-respect des consignes	PER_10	BCO_RPS.2.1
PER_DEV	38	Personnel utilisateur peu ou mal formé	PER_12	BSP_FOU.2.1
PER_DEV	38	Absence de documentation d'utilisation des applicatifs existantes	PER_12	CDO_APP.1.1
PER_DEV	38	Non-respect des consignes	PER_10	BSP_RIS.5.1
PER_DEV	38	Manque de professionnalisme	PER_05	CPS_PAQ.2.2
PER_DEV	38	Personnel peu habitué à la saisie	PER_06	CPS_PAQ.3.1
PER_DEV	38	Personnel peu habitué à la saisie	PER_06	BSP_FOU.2.1
PER_DEV	38	Non-respect des consignes	PER_10	BSP_SPR.4.1
PER_DEV	38	Non-respect des consignes	PER_10	BSP_SPR.1.1
PER_DEV	38	Conditions de travail défavorables	ORG_45	CRH_CDT.1.2
PER_DEV	38	Non-respect des consignes	PER_10	BSP_RIS.5.2
PER_DEV	41	Responsabilité de chacun non connue	PER_05	BOS_ISI.3.1
PER_DEV	41	Responsabilité de chacun non connue	PER_05	BPS_PSI.1.3
PER_DEV	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.1.1
PER_DEV	41	Responsabilité de chacun non connue	PER_05	BSP_SPR.4.1
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_DDE.1.1
PER_DEV	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.5
PER_DEV	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.4
PER_DEV	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.3
PER_DEV	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.2
PER_DEV	42	Indisponibilité causée par la maladie	PER_04	CRH_DDE.1.1
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.5
PER_DEV	42	Indisponibilité causée par la maladie	PER_04	CRH_DDE.1.2
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_DDE.1.2
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CRH_PDP.1.1
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.1
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.2
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.3
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)	PER_04	CFO_FRS.1.4
PER_DEV	42	Indisponibilité causée par la maladie	PER_04	CFO_FRS.1.1

4.5 PHY : Site

4.5.1 PHY_LIE : Lieu

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE	14	Aucune prise en compte de risque des rayonnements électromagnétiques ou thermiques à la conception	PHY_03	BPE_SEM.2.1
PHY_LIE	14	Proximité d'une source de rayonnements électromagnétiques ou thermiques	PHY_03	CIS_ADL.2.2
PHY_LIE	15	Aucune prise en compte de risque des rayonnements électromagnétiques ou thermiques à la conception	PHY_03	BPE_SEM.2.1
PHY_LIE	15	Proximité d'une source de rayonnements électromagnétiques ou thermiques	PHY_03	CIS_ADL.2.2
PHY_LIE	16	Proximité d'une source de rayonnements électromagnétiques ou thermiques	PHY_03	CIS_ADL.2.2
PHY_LIE	16	Aucune prise en compte de risque des rayonnements électromagnétiques ou thermiques à la conception	PHY_03	BPE_SEM.2.1
PHY_LIE	17	Absence de réalisation de zonage TEMPEST	PHY_05	BPE_SEM.3.1

4.5.1.1 PHY_LEI.1 : Externe

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.1	2	Site placé dans une zone inondable	PHY_04	CIS_SSI.1.2
PHY_LIE.1	3	Proximité de sources de pollution (source sonore, fumée, vapeur…)	PHY_04	CIS_SSI.1.2
PHY_LIE.1	4	Proximité d'activité industrielle ou de site à risque	PHY_04	CRR_ETU.1.1
PHY_LIE.1	4	Proximité d'activité industrielle ou de site à risque	PHY_04	CIS_SSI.1.2
PHY_LIE.1	4	Proximité d'activité industrielle ou de site à risque	PHY_04	CRR_ETU.2.2
PHY_LIE.1	4	Proximité d'activité industrielle ou de site à risque	PHY_04	CRR_ETU.2.1
PHY_LIE.1	4	Proximité d'activité industrielle ou de site à risque	PHY_04	CRR_ETU.1.2
PHY_LIE.1	4	Possibilités de destruction causée par un événements extérieurs (collisions, attentats)	PHY_04	CRR_ETU.2.2
PHY_LIE.1	4	Possibilités de destruction causée par un événements extérieurs (collisions, attentats)	PHY_04	CRR_ETU.2.1
PHY_LIE.1	4	Possibilités de destruction causée par un événements extérieurs (collisions, attentats)	PHY_04	CRR_ETU.1.2
PHY_LIE.1	4	Possibilités de destruction causée par un événements extérieurs (collisions, attentats)	PHY_04	CRR_ETU.1.1
PHY_LIE.1	4	Possibilités de destruction causée par un événements extérieurs (collisions, attentats)	PHY_04	CIS_SSI.1.3
PHY_LIE.1	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.1	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.1	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.1	8	Site recensé comme à risque	PHY_04	CRR_ETU.2.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.1	8	Site recensé comme à risque	PHY_04	CRR_ETU.1.1
PHY_LIE.1	8	Site recensé comme à risque	PHY_04	CIS_SSI.1.2
PHY_LIE.1	8	Site recensé comme à risque	PHY_04	CRR_ETU.2.1
PHY_LIE.1	8	Site recensé comme à risque	PHY_04	CRR_ETU.1.2
PHY_LIE.1	9	Site dans lequel des phénomènes météorologiques extrêmes se produisent périodiquement (tempête, ouragan, cyclone…)	PHY_04	CIS_CDL.1.1
PHY_LIE.1	9	Site dans lequel des phénomènes météorologiques extrêmes se produisent périodiquement (tempête, ouragan, cyclone…)	PHY_04	CIS_SSI.1.2
PHY_LIE.1	9	Site dans lequel des phénomènes météorologiques extrêmes se produisent périodiquement (tempête, ouragan, cyclone…)	PHY_04	CIS_SSI.1.1
PHY_LIE.1	10	Site placé dans une zone inondable	PHY_04	CIS_SSI.1.2
PHY_LIE.1	18	Présence de lieu d'observation à l'extérieur du site	PHY_02	BPE_SEM.3.1
PHY_LIE.1	18	Présence de lieu d'observation à l'extérieur du site	PHY_02	CIS_ADL.1.1
PHY_LIE.1	19	Possibilité de capter les transmissions depuis l'extérieur du site	PHY_05	BGC_GER.1.1
PHY_LIE.1	19	Possibilité de capter les transmissions depuis l'extérieur du site	PHY_05	BPE_SEM.3.1
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site	PER_01	BGC_EIL.1.1
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site	PER_01	BGC_EIL.2.1
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site	PER_01	BGC_EIL.5.1
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site	PER_01	BGC_EIL.7.1
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site	PER_01	BGC_EIL.4.1
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site	PER_01	BGC_MSS.1.1
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site	PER_01	BGC_EIL.6.1
PHY_LIE.1	21	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BMA_IMT.1.1
PHY_LIE.1	21	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BMA_IMT.2.1
PHY_LIE.1	21	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BPE_SEM.5.1
PHY_LIE.1	22	Présence de support mis au rebut à l'extérieur du site	ORG_15	BPE_SEM.6.1
PHY_LIE.1	22	Présence de support mis au rebut à l'extérieur du site	ORG_15	CGS_GMR.1.1
PHY_LIE.1	22	Présence de support mis au rebut à l'extérieur du site	ORG_15	CGS_GMR.1.2
PHY_LIE.1	25	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BPE_SEM.5.1
PHY_LIE.1	25	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BMA_IMT.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.1	25	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BMA_IMT.1.1
PHY_LIE.1	26	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BMA_IMT.1.1
PHY_LIE.1	26	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BPE_SEM.5.1
PHY_LIE.1	26	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)	PER_01	BMA_IMT.2.1
PHY_LIE.1	42	Climat social difficile pouvant provoquer des grèves de transport	PHY_04	CRH_PDP.1.1
PHY_LIE.1	42	Climat social difficile pouvant provoquer des grèves de transport	PHY_04	CIS_SSI.1.4
PHY_LIE.1	42	Climat social difficile pouvant provoquer des grèves de transport	PHY_04	CRH_PDP.1.3

4.5.1.2 PHY_LEI.2 : Locaux

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.2	1	Absence de cloisonnement anti-feu	PHY_09	CIS_CSI.1.1
PHY_LIE.2	1	Vieillissement des locaux	PHY_10	CIS_CSI.2.1
PHY_LIE.2	1	Absence de contrôle d'accès au site ou aux locaux	PHY_03	CET_EGT.1.1
PHY_LIE.2	1	Présence d'ouverture sur la voie publique (fenêtre)	PHY_03	CIS_ADL.1.2
PHY_LIE.2	1	Absence de cloisonnement anti-feu	PHY_09	CIS_CSI.1.2
PHY_LIE.2	1	Absence de cloisonnement anti-feu	PHY_09	CIS_MPP.2.1
PHY_LIE.2	1	Absence de contrôle d'accès au site ou aux locaux	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	2	Absence de contrôle des accès physiques aux locaux	PHY_03	CET_EGT.1.1
PHY_LIE.2	2	Ouverture à l'extérieur non étanche	PHY_03	CIS_MPP.3.3
PHY_LIE.2	2	Présence d'un dispositif d'extinction incendie à eau	PHY_03	CIS_MPP.2.2
PHY_LIE.2	2	Absence de contrôle des accès physiques aux locaux	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	3	Atmosphère polluée (hangar, atelier…)	PHY_04	CIS_ADL.2.1
PHY_LIE.2	3	Proximité de sources de pollution (source sonore, fumée, vapeur…)	PHY_04	CIS_SSI.1.2
PHY_LIE.2	4	Locaux dans lesquels les risques d'explosion/implosion n'ont pas été pris en compte	PHY_03	CEI_ERS.1.1
PHY_LIE.2	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.2	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.2	6	Non prise en compte des conditions climatiques dans la construction des locaux	PHY_04	CIS_CDL.1.1
PHY_LIE.2	6	Absence de moyens de ventilation ou de climatisation lors de chaleur estivale excessive	PHY_01	CIS_ADL.2.1
PHY_LIE.2	7	Non prise en compte des risques sismiques dans la construction des bâtiments	PHY_04	CIS_CDL.1.1
PHY_LIE.2	8	Non prise en compte des risques sismiques dans la construction des bâtiments	PHY_04	CIS_CDL.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.2	9	Absence de protection contre la foudre	PHY_04	CIS_CDL.1.1
PHY_LIE.2	10	Absence de protection contre la montée des eaux	PHY_03	CIS_SSI.1.2
PHY_LIE.2	10	Absence de protection contre la montée des eaux	PHY_03	CIS_MPP.3.4
PHY_LIE.2	17	Accès public à proximité des bâtiments	PHY_05	BPE_SEM.3.1
PHY_LIE.2	17	Accès public à proximité des bâtiments	PHY_05	BPE_ZOS.4.1
PHY_LIE.2	17	Accès public à proximité des bâtiments	PHY_05	CIS_ADL.1.1
PHY_LIE.2	17	Accès public à proximité des bâtiments	PHY_05	BPE_ZOS.1.1
PHY_LIE.2	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.2	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.2	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.2	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.2	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.2	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.2	22	Présence de support mis au rebut dans des locaux publics	ORG_15	BPE_SEM.6.1
PHY_LIE.2	22	Présence de support mis au rebut dans des locaux publics	ORG_15	CGS_GMR.1.2
PHY_LIE.2	22	Présence de support mis au rebut dans des locaux publics	ORG_15	CGS_GMR.1.1
PHY_LIE.2	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.1.1
PHY_LIE.2	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.3.1
PHY_LIE.2	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.2.1
PHY_LIE.2	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BGC_INT.2.1
PHY_LIE.2	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.2	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.2	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.2	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.2	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.2	28	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel…)	PHY_10	CIS_ADL.2.1
PHY_LIE.2	29	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel…)	PHY_10	CIS_ADL.2.1
PHY_LIE.2	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.2	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.2	33	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.2	33	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.2	33	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.2	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.2	33	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.2	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.2	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.2	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.2	34	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.2	34	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.2	34	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.2	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.2	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.2	34	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.2	35	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.2	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.2	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.2	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.2	35	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.2	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.2	35	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.2	35	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.2	36	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.2	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.2	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.2	36	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.2	36	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.2	36	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.2	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.2	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.2	38	Environnement de travail défavorable (locaux trop petits, manque d'espace de rangement…)	PHY_12	CRH_CDT.1.1
PHY_LIE.2	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.2	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.2	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.2	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.2	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.2	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.2	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.2	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.2	41	Absence d'historisation des entrées et sorties des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.2	41	Absence d'historisation des entrées et sorties des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.2	41	Absence d'historisation des entrées et sorties des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.2	42	Personnels spécialisés hébergés dans des locaux distants	PHY_04	CRH_PDP.1.3
PHY_LIE.2	42	Personnels spécialisés hébergés dans des locaux distants	PHY_04	CRH_PDP.1.1
PHY_LIE.2	42	Personnels spécialisés hébergés dans des locaux distants	PHY_04	CRH_PDP.1.2
PHY_LIE.2	42	Personnels spécialisés hébergés dans des locaux distants	PHY_04	CIS_SSI.1.4
PHY_LIE.2	42	Personnels habitant loin des locaux	PHY_04	CRH_PDP.1.3
PHY_LIE.2	42	Personnels habitant loin des locaux	PHY_04	CIS_SSI.1.4

4.5.1.3 PHY_LIE.3 : Zone

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.3	1	Absence ou mauvais dimensionnement ou inadéquation du dispositif d'extinction automatique d'incendie	PHY_09	CIS_MPP.2.2
PHY_LIE.3	1	Absence de prise en compte dans la phase d'installation des risques d'incendie spécifiques aux équipements hébergés	PHY_06	CEI_ERS.1.1
PHY_LIE.3	1	Présence d'ouverture sur la voie publique (fenêtre)	PHY_03	CIS_ADL.1.2
PHY_LIE.3	2	Canalisation d'eau à proximité des équipements de terminaison	PHY_03	CIS_MPP.3.2
PHY_LIE.3	2	Canalisation d'eau à proximité des équipements de terminaison	PHY_03	CIS_ADL.2.2
PHY_LIE.3	2	Absence de puisard	PHY_03	CIS_MPP.3.1
PHY_LIE.3	2	Absence d'identification claire des vannes de coupure d'eau	PHY_07	CIS_ADL.3.1
PHY_LIE.3	2	Accès non protégé	PHY_03	BPE_ZOS.2.1
PHY_LIE.3	2	Accès non protégé	PHY_03	BPE_ZOS.5.1
PHY_LIE.3	2	Canalisation d'eau à proximité des équipements	PHY_03	CIS_MPP.3.2
PHY_LIE.3	2	Dispositif d'extinction incendie à eau	PHY_10	CIS_MPP.2.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.3	2	Plafond ou ouverture à l'extérieur non étanche	PHY_03	CIS_MPP.3.3
PHY_LIE.3	2	Plafond ou ouverture à l'extérieur non étanche	PHY_03	CIS_MPP.3.3
PHY_LIE.3	2	Canalisation d'eau à proximité des équipements	PHY_03	CIS_ADL.2.2
PHY_LIE.3	4	Locaux dans lesquels les risques d'explosion/implosion n'ont pas été pris en compte	PHY_03	CEI_ERS.1.1
PHY_LIE.3	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports	PHY_03	CIS_ZOS.1.1
PHY_LIE.3	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports	PHY_03	BPE_ZOS.2.1
PHY_LIE.3	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports	PHY_03	BPE_ZOS.1.1
PHY_LIE.3	6	Absence de moyens de ventilation ou de climatisation lors de chaleur estivale excessive	PHY_01	CIS_ADL.2.1
PHY_LIE.3	6	Non prise en compte des conditions climatiques dans la construction des locaux	PHY_04	CIS_CDL.1.1
PHY_LIE.3	9	Absence de protection contre la foudre	PHY_04	CIS_CDL.1.1
PHY_LIE.3	10	Absence de protection contre la montée des eaux	PHY_03	CIS_MPP.3.4
PHY_LIE.3	10	Absence de protection contre la montée des eaux	PHY_03	CIS_SSI.1.2
PHY_LIE.3	11	Absence de révision des besoins de climatisation en cas de modification des locaux ou d'ajout de matériel	PHY_01	CDS_DES.1.2
PHY_LIE.3	11	Absence de révision des besoins de climatisation en cas de modification des locaux ou d'ajout de matériel	PHY_01	CDS_DES.1.1
PHY_LIE.3	17	Salle située à proximité de la voie publique	PHY_05	BPE_SEM.3.1
PHY_LIE.3	17	Salle située à proximité de la voie publique	PHY_05	CIS_ADL.1.1
PHY_LIE.3	17	Salle située à proximité de la voie publique	PHY_05	BPE_ZOS.1.1
PHY_LIE.3	17	Salle située à proximité de la voie publique	PHY_05	CIS_ADL.1.2
PHY_LIE.3	17	Salle située à proximité de la voie publique	PHY_05	BPE_ZOS.4.1
PHY_LIE.3	18	Zone observable depuis un lieu de passage	PHY_07	BPE_ZOS.4.1
PHY_LIE.3	18	Zone observable depuis un lieu de passage	PHY_07	BPE_ZOS.1.1
PHY_LIE.3	18	Zone observable depuis un lieu de passage	PHY_07	CIS_ADL.1.1
PHY_LIE.3	18	Zone observable depuis un lieu de passage	PHY_07	BPE_SEM.3.1
PHY_LIE.3	18	Zone disposant d'ouverture sur la voie publique	PHY_02	CIS_ADL.1.2
PHY_LIE.3	18	Zone disposant d'ouverture sur la voie publique	PHY_02	BPE_SEM.3.1
PHY_LIE.3	18	Zone disposant d'ouverture sur la voie publique	PHY_02	BPE_ZOS.4.1
PHY_LIE.3	18	Zone disposant d'ouverture sur la voie publique	PHY_02	BPE_ZOS.1.1
PHY_LIE.3	18	Zone disposant d'ouverture sur la voie publique	PHY_02	CIS_ADL.1.1
PHY_LIE.3	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.3	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.3	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.3	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.3	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.3	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.3	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.3	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.3	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.3	22	Présence de support mis au rebut dans des zones accessibles à des personnes n'ayant pas le besoin d'en connaître	ORG_15	CGS_GMR.1.2
PHY_LIE.3	22	Présence de support mis au rebut dans des zones accessibles à des personnes n'ayant pas le besoin d'en connaître	ORG_15	BPE_SEM.6.1
PHY_LIE.3	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.1.1
PHY_LIE.3	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BGC_INT.2.1
PHY_LIE.3	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.2.1
PHY_LIE.3	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.3.1
PHY_LIE.3	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.3	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.3	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.3	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_LIE.3	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_LIE.3	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_LIE.3	28	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel…)	PHY_10	CIS_ADL.2.1
PHY_LIE.3	29	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel…)	PHY_10	CIS_ADL.2.1
PHY_LIE.3	33	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.3	33	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.3	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.3	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.3	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.3	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.3	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	33	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	33	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.3	33	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.3	33	Absence de journalisation des entrées des personnes	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.3	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	34	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.3	34	Absence de journalisation des entrées des personnes	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	34	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.3	34	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.3	34	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.3	34	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.3	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.3	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.3	35	Absence de journalisation des entrées des personnes	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	35	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.3	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.3	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.3	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.3	35	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.3	35	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.3	35	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.3	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.3	35	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.3	36	Absence de journalisation des entrées des personnes	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.3	36	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.3	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.3	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	36	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	CET_EGT.1.3
PHY_LIE.3	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.3	36	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.5
PHY_LIE.3	36	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	36	Absence de journalisation des entrées des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.3	38	Environnement de travail défavorable (locaux trop petit, manque d'espace de rangement…)	PHY_12	CRH_CDT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_LIE.3	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.3	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.3	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.3	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.3	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.3
PHY_LIE.3	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.2
PHY_LIE.3	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.1
PHY_LIE.3	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	CET_EGT.3.4
PHY_LIE.3	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	41	Absence d'historisation des entrées et sorties des personnes	PHY_07	CET_EGT.3.5
PHY_LIE.3	41	Absence d'historisation des entrées et sorties des personnes	PHY_07	CET_EGT.1.6
PHY_LIE.3	41	Absence d'historisation des entrées et sorties des personnes	PHY_07	BPE_ZOS.2.1
PHY_LIE.3	41	Absence d'historisation des entrées et sorties des personnes	PHY_07	CET_EGT.1.5

4.5.2 PHY_SRV : Service essentiel

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV	4	Locaux dans lesquels les risques d'explosion/implosion n'ont pas été pris en compte	PHY_03	CEI_ERS.1.1
PHY_SRV	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports	PHY_03	CIS_ZOS.1.1
PHY_SRV	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports	PHY_03	BPE_ZOS.2.1
PHY_SRV	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports	PHY_03	BPE_ZOS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV	10	Absence de protection contre la montée des eaux	PHY_03	CIS_MPP.3.4
PHY_SRV	10	Absence de protection contre la montée des eaux	PHY_03	CIS_SSI.1.2
PHY_SRV	14	Aucune prise en compte des risques liés à la proximité d'une source électromagnétique	PHY_03	CEI_ERS.1.1
PHY_SRV	15	Aucune prise en compte des risques liés à la proximité d'une source électromagnétique	PHY_03	CEI_ERS.1.1
PHY_SRV	16	Aucune prise en compte des risques liés à la proximité d'une source électromagnétique	PHY_03	CEI_ERS.1.1
PHY_SRV	28	Déclenchement manuel de la solution de secours	ORG_16	CGS_GSS.2.1
PHY_SRV	28	Déclenchement manuel de la solution de secours	ORG_16	BSP_RIS.1.1
PHY_SRV	28	Déclenchement manuel de la solution de secours	ORG_16	CGS_GSS.2.2
PHY_SRV	28	Absence de contrôle du bon fonctionnement des ressources de secours	ORG_16	CGS_GMA.1.1
PHY_SRV	28	Déclenchement manuel de la solution de secours	ORG_16	BGC_PRE.3.1
PHY_SRV	28	Absence de contrôle du bon fonctionnement des ressources de secours	ORG_16	CGS_GMA.1.2
PHY_SRV	29	Déclenchement manuel de la solution de secours	ORG_16	BGC_PRE.3.1
PHY_SRV	29	Déclenchement manuel de la solution de secours	ORG_16	BSP_RIS.1.1
PHY_SRV	29	Déclenchement manuel de la solution de secours	ORG_16	CGS_GSS.2.1
PHY_SRV	29	Déclenchement manuel de la solution de secours	ORG_16	CGS_GSS.2.2
PHY_SRV	29	Absence de contrôle du bon fonctionnement des ressources de secours	ORG_16	CGS_GMA.1.1
PHY_SRV	29	Absence de contrôle du bon fonctionnement des ressources de secours	ORG_16	CGS_GMA.1.2

4.5.2.1 PHY_SRV.1 : Communication

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.1	1	Absence ou mauvais dimensionnement ou inadéquation du dispositif d'extinction automatique d'incendie	PHY_09	CIS_MPP.2.2
PHY_SRV.1	1	Absence de prise en compte dans la phase d'installation des risques d'incendie spécifiques aux équipements hébergés	PHY_06	CEI_ERS.1.1
PHY_SRV.1	1	Présence d'ouverture sur la voie publique (fenêtre)	PHY_03	CIS_ADL.1.2
PHY_SRV.1	2	Canalisation d'eau à proximité des équipements de terminaison	PHY_03	CIS_ADL.2.2
PHY_SRV.1	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels	PHY_03	BPE_ZOS.2.1
PHY_SRV.1	2	Câblage posé sur le sol	PHY_07	CIS_CSI.1.1
PHY_SRV.1	2	Canalisation d'eau à proximité des équipements de terminaison	PHY_03	CIS_MPP.3.2
PHY_SRV.1	2	Plafond ou ouverture à l'extérieur non étanche	PHY_03	CIS_MPP.3.3
PHY_SRV.1	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels	PHY_03	CIS_MPP.1.2
PHY_SRV.1	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels	PHY_03	CIS_ZOS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.1	12	Equipement terminal de communication ne disposant pas d'alimentation secourue	PHY_01	CGS_GSS.1.1
PHY_SRV.1	13	Absence de maintenance des équipements de terminaison et de distribution	PHY_01	CGS_GMA.3.2
PHY_SRV.1	13	Absence de maintenance des équipements de terminaison et de distribution	PHY_01	CGS_GMA.3.3
PHY_SRV.1	13	Absence de maintenance des équipements de terminaison et de distribution	PHY_01	CGS_GMA.3.1
PHY_SRV.1	13	Absence de maintenance des équipements de terminaison et de distribution	PHY_01	BPE_SEM.4.1
PHY_SRV.1	13	Défauts d'exploitation du réseau téléphonique interne	PHY_01	BSP_FOU.2.1
PHY_SRV.1	13	Dysfonctionnement déjà constaté dans la fourniture du service de télécommunication	PHY_01	BGC_PRE.6.1
PHY_SRV.1	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication	PHY_03	CIS_MPP.1.2
PHY_SRV.1	13	Absence de maintenance des équipements de terminaison et de distribution	PHY_01	CGS_GMA.1.2
PHY_SRV.1	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication	PHY_03	BPE_ZOS.2.1
PHY_SRV.1	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication	PHY_03	CIS_ZOS.1.1
PHY_SRV.1	13	Absence de maintenance des équipements de terminaison et de distribution	PHY_01	CGS_GMA.1.1
PHY_SRV.1	17	Absence de prise en compte des règles d'installation	PHY_10	CCS_RGI.1.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	CGS_PDI.1.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	FPT_PHP.1/2.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	FPT_PHP.2.3
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	BOS_SAT.1.2
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.5.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.1.1
PHY_SRV.1	17	Support facilitant la capture des signaux parasites compromettants (câbles électriques, tuyauteries…)	PHY_05	BPE_SEM.3.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.2.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.3.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.4.1
PHY_SRV.1	17	Absence de protection des accès aux équipements	PHY_03	BPE_SEM.1.1
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication	RES_01	BPE_ZOS.2.1
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication	RES_01	BMA_MAA.2.1
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication	RES_01	BMA_MAR.3.1
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication	RES_01	BMA_MAR.4.1
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication	RES_01	BMA_MAS.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication	RES_01	BMA_REU.2.1
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication	RES_01	CET_EGT.1.1
PHY_SRV.1	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BGC_INT.2.1
PHY_SRV.1	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.3.1
PHY_SRV.1	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.2.1
PHY_SRV.1	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur	PHY_07	BMA_SAS.1.1
PHY_SRV.1	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_SRV.1	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_SRV.1	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_SRV.1	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	BPE_ZOS.5.1
PHY_SRV.1	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CIS_ADL.2.1
PHY_SRV.1	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects	PHY_03	CET_EGT.1.1
PHY_SRV.1	30	Mauvais dimensionnement des ressources Télécom par exemple suite à l'exploitation au quotidien de ressources destinées à la solution de secours	ORG_16	CGS_GSS.1.4
PHY_SRV.1	33	Absence de sécurisation des lignes et équipements de communication	PHY_07	BGC_GER.1.1
PHY_SRV.1	36	Absence de sécurisation des lignes et équipements de communication	PHY_07	BGC_GER.1.1
PHY_SRV.1	38	Absence d'étiquetage des câbles ou de plan de câblage	PHY_11	CIS_ADL.3.1
PHY_SRV.1	38	Absence d'étiquetage des câbles ou de plan de câblage	PHY_11	CIS_CSI.1.1
PHY_SRV.1	38	Insuffisance d'espace des locaux techniques	PHY_12	CIS_ADL.2.3

4.5.2.2 PHY_SRV.2 : Énergie

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.2	1	Absence ou mauvais dimensionnement ou inadéquation du dispositif d'extinction automatique d'incendie	PHY_09	CIS_MPP.2.2
PHY_SRV.2	1	Présence d'ouverture sur la voie publique (fenêtre)	PHY_03	CIS_ADL.1.2
PHY_SRV.2	1	Absence de prise en compte dans la phase d'installation des risques d'incendie spécifiques aux équipements hébergés	PHY_06	CEI_ERS.1.1
PHY_SRV.2	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels	PHY_03	CIS_ZOS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.2	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels	PHY_03	CIS_MPP.1.2
PHY_SRV.2	2	Câblage posé sur le sol	PHY_07	CIS_CSI.1.1
PHY_SRV.2	2	Plafond ou ouverture à l'extérieur non étanche	PHY_03	CIS_MPP.3.3
PHY_SRV.2	2	Canalisation d'eau à proximité des équipements de terminaison	PHY_03	CIS_MPP.3.2
PHY_SRV.2	2	Canalisation d'eau à proximité des équipements de terminaison	PHY_03	CIS_ADL.2.2
PHY_SRV.2	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels	PHY_03	BPE_ZOS.2.1
PHY_SRV.2	12	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques	PHY_03	BPE_ZOS.2.1
PHY_SRV.2	12	Absence d'analyse de la puissance énergétique de secours nécessaire en cas d'ajout de matériel	PHY_01	CGS_GSS.1.2
PHY_SRV.2	12	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques	PHY_03	CIS_ZOS.1.1
PHY_SRV.2	12	Le poste de transformation moyenne tension / basse tension n'est pas implanté sur le site (avec accès contrôlé du fournisseur)	PHY_01	CIS_MPP.1.2
PHY_SRV.2	12	Le poste de transformation moyenne tension / basse tension n'est pas implanté sur le site (avec accès contrôlé du fournisseur)	PHY_01	CIS_MPP.1.3
PHY_SRV.2	12	Le tableau général basse tension n'est pas accessible	PHY_01	CIS_MPP.1.1
PHY_SRV.2	12	Les divers revêtements de sols ou muraux ne sont pas anti-statiques	PHY_03	BPE_SEM.2.1
PHY_SRV.2	12	Les locaux renfermant des batteries dont la composition est à base d'acide ne sont pas dédiés et isolés physiquement des matériels auxquels ils sont raccordés	PHY_06	CEI_ERS.1.1
PHY_SRV.2	12	Les masses et terres ne sont pas conformes à la réglementation	PHY_10	CIS_CSI.1.1
PHY_SRV.2	12	Mauvais dimensionnement des dispositifs de secours énergie (onduleur, batteries…)	PHY_01	CDS_DES.1.1
PHY_SRV.2	12	Mauvais dimensionnement des dispositifs de secours énergie (onduleur, batteries…)	PHY_01	CDS_DES.1.2
PHY_SRV.2	12	Les locaux renfermant des batteries dont la composition est à base d'acide ne sont pas munis de ventilation mécanique et aménagés électriquement en antidéflagrant	PHY_06	CEI_ERS.1.1
PHY_SRV.2	12	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques	PHY_03	CIS_MPP.1.2
PHY_SRV.2	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication	PHY_03	CIS_MPP.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.2	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication	PHY_03	BPE_ZOS.2.1
PHY_SRV.2	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication	PHY_03	CIS_ZOS.1.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	FPT_PHP.3.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	BOS_SAT.1.2
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	BPE_SEM.1.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.5.1
PHY_SRV.2	17	Support facilitant la capture des signaux parasites compromettants (câbles électriques, tuyauteries…)	PHY_05	BPE_SEM.3.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.1.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.2.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.4.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	FPT_PHP.2.3
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	FPT_PHP.1/2.1
PHY_SRV.2	17	Absence de prise en compte des règles d'installation	PHY_10	CCS_RGI.1.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	CGS_PDI.1.1
PHY_SRV.2	17	Absence de protection des accès aux équipements	PHY_03	BPE_ZOS.3.1
PHY_SRV.2	30	Mauvais dimensionnement des ressources de secours	ORG_16	CGS_GSS.1.3
PHY_SRV.2	38	Absence de procédure d'exploitation	ORG_04	BGC_PRE.1.1

4.5.2.3 PHY_SRV.3 : Refroidissement /pollution

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.3	1	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.2
PHY_SRV.3	1	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.1.2
PHY_SRV.3	1	Absence de maintenance des équipements de climatisation	ORG_27	BPE_SEM.4.1
PHY_SRV.3	1	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.1.1
PHY_SRV.3	1	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.1
PHY_SRV.3	1	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.3
PHY_SRV.3	2	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.1.2
PHY_SRV.3	2	Vieillissement des canalisations de refroidissement	PHY_10	CGS_GMA.1.1
PHY_SRV.3	2	Absence de vanne d'arrêt d'eau	PHY_07	CIS_MPP.1.1
PHY_SRV.3	2	Absence de maintenance des équipements de climatisation	ORG_27	BPE_SEM.4.1
PHY_SRV.3	2	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.3
PHY_SRV.3	2	Vieillissement des canalisations de refroidissement	PHY_10	CGS_GMA.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.3	2	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.1
PHY_SRV.3	2	Vieillissement des canalisations de refroidissement	PHY_10	BPE_SEM.4.1
PHY_SRV.3	2	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.1.1
PHY_SRV.3	2	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.2
PHY_SRV.3	3	Absence de maintenance des équipements de climatisation	ORG_27	BPE_SEM.4.1
PHY_SRV.3	3	Accès non protégé aux équipements	PHY_03	BPE_ZOS.2.1
PHY_SRV.3	3	Accès non protégé aux équipements	PHY_03	CIS_ZOS.1.1
PHY_SRV.3	3	Accès non protégé aux équipements	PHY_03	CIS_MPP.1.2
PHY_SRV.3	3	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.3
PHY_SRV.3	3	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.2
PHY_SRV.3	3	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.3.1
PHY_SRV.3	3	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.1.1
PHY_SRV.3	3	Vieillissement des filtres de climatisation	PHY_10	CGS_GMA.3.1
PHY_SRV.3	3	Absence de maintenance des équipements de climatisation	ORG_27	CGS_GMA.1.2
PHY_SRV.3	3	Vieillissement des filtres de climatisation	PHY_10	CGS_GMA.1.1
PHY_SRV.3	3	Vieillissement des filtres de climatisation	PHY_10	CGS_GMA.3.2
PHY_SRV.3	3	Vieillissement des filtres de climatisation	PHY_10	CGS_GMA.3.3
PHY_SRV.3	3	Vieillissement des filtres de climatisation	PHY_10	BPE_SEM.4.1
PHY_SRV.3	3	Vieillissement des filtres de climatisation	PHY_10	CGS_GMA.1.2
PHY_SRV.3	11	Absence de matériel redondant suffisamment dimensionné	PHY_01	CGS_GSS.1.2
PHY_SRV.3	11	Dispositif dépendant d'un fournisseur en eau glacé ou alimentation	PHY_01	BGC_PRE.6.1
PHY_SRV.3	11	Accès non protégé aux dispositifs d'alimentation en eau et énergie	PHY_03	CIS_ZOS.1.1
PHY_SRV.3	11	Accès non protégé aux dispositifs d'alimentation en eau et énergie	PHY_03	CIS_MPP.1.2
PHY_SRV.3	11	Accès non protégé aux dispositifs d'alimentation en eau et énergie	PHY_03	BPE_ZOS.2.1
PHY_SRV.3	11	Absence de matériel redondant suffisamment dimensionné	PHY_01	CGS_GSS.1.1
PHY_SRV.3	11	Absence de maintenance des équipements de climatisation	PHY_01	BPE_SEM.4.1
PHY_SRV.3	11	Absence de maintenance des équipements de climatisation	PHY_01	CGS_GMA.3.2
PHY_SRV.3	11	Absence de maintenance des équipements de climatisation	PHY_01	CGS_GMA.3.1
PHY_SRV.3	11	Absence de maintenance des équipements de climatisation	PHY_01	CGS_GMA.1.2
PHY_SRV.3	11	Absence de maintenance des équipements de climatisation	PHY_01	CGS_GMA.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
PHY_SRV.3	11	Absence de maintenance des équipements de climatisation	PHY_01	CGS_GMA.3.3
PHY_SRV.3	11	Dispositif non suffisamment dimensionné par rapport aux besoins	PHY_01	CDS_DES.1.2
PHY_SRV.3	11	Dispositif non suffisamment dimensionné par rapport aux besoins	PHY_01	CDS_DES.1.1
PHY_SRV.3	30	Mauvais dimensionnement des ressources de secours	ORG_16	CGS_GSS.1.3
PHY_SRV.3	38	Absence de procédure d'exploitation	ORG_04	BGC_PRE.1.1

4.6 ORG : Organisation

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG	1	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.2.2
ORG	1	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.2
ORG	1	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.1
ORG	2	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.2.2
ORG	2	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.2
ORG	2	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.1
ORG	34	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_41	BPS_PSI.1.3
ORG	34	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.5.1
ORG	34	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.1.1
ORG	34	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.2.1

4.6.1 ORG_DEP : Organisation dont dépend l'organisme

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_22	CCS_SIN.3.3
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_22	CIS_CSI.1.3
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.2.1
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CCS_CSP.1.2
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.2.3
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CCS_CSP.1.3
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_22	CCS_SSE.1.1
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	BOS_SAT.2.1
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.2.2
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CCS_CSP.1.4
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.1.2
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.1.6
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.1.5
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.1.4
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CET_EGT.1.3
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)	ORG_25	CCS_CSP.2.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	4	Absence de service d'urgence proche de l'organisme	ORG_24	CIS_SSI.1.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	6	Absence de service d'urgence proche de l'organisme	ORG_24	CIS_SSI.1.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	7	Absence de service d'urgence proche de l'organisme	ORG_24	CIS_SSI.1.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	8	Absence de service d'urgence proche de l'organisme	ORG_24	CIS_SSI.1.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	9	Absence de service d'urgence proche de l'organisme	ORG_24	CIS_SSI.1.1
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	10	Absence de service d'urgence proche de l'organisme	ORG_24	CIS_SSI.1.1
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.1
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_CSI.1.2
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.1
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_SOT.1.2
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.2
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	CIS_PSI.1.3
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BCO_RPS.1.2
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_23	BPE_ZOS.1.1
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	CRI_MOF.2.1
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme	ORG_38	BOS_ISI.7.1
ORG_DEP	17	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_DEP	17	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1
ORG_DEP	17	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_DEP	17	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1
ORG_DEP	17	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_DEP	17	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.1.2
ORG_DEP	17	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2
ORG_DEP	17	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.2.1
ORG_DEP	18	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BCM_CLI.1.1
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BCM_CLI.1.2
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BCM_CLI.2.1
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_EIL.2.1
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_EIL.4.1
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_EIL.7.1
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_GER.1.1
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BPS_PSI.1.5
ORG_DEP	18	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	CGS_PDI.1.1
ORG_DEP	18	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_ZOS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	18	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_ZOS.4.1
ORG_DEP	18	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_ZOS.3.1
ORG_DEP	18	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_SEM.3.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	FPT_PHP.1/2.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_SEM.3.2
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_ZOS.5.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_ZOS.2.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_ZOS.3.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_ZOS.4.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	CGS_PDI.1.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BOS_SAT.1.2
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	BPE_SEM.1.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	FPT_PHP.2.3
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BCM_CLI.1.1
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BCM_CLI.1.2
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BCM_CLI.2.1
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_EIL.2.1
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_EIL.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_EIL.7.1
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel	ORG_15	BGC_EIL.7.1
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_30	FPT_PHP.3.1
ORG_DEP	20	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.2.1
ORG_DEP	20	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.1.2
ORG_DEP	20	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.1.1
ORG_DEP	20	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BGC_MSS.3.1
ORG_DEP	20	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BPS_PSI.1.5
ORG_DEP	20	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	BPE_ZOS.1.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	CGS_PDI.1.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	FPT_PHP.1/2.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	FPT_PHP.2.3
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	BPE_ZOS.5.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	BPE_SEM.1.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	BPE_ZOS.2.1
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	BPE_ZOS.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_02	BPE_ZOS.4.1
ORG_DEP	22	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_DEP	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_DEP	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	FDP_RIP.1.1
ORG_DEP	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	BPE_SEM.6.1
ORG_DEP	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	BGC_MSS.2.1
ORG_DEP	22	Absence de contrôle des biens sensibles	ORG_04	BCM_RLC.1.1
ORG_DEP	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_DEP	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_DEP	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	FDP_RIP.2.1
ORG_DEP	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_DEP	22	Absence de contrôle des biens sensibles	ORG_04	BMA_IMT.2.1
ORG_DEP	22	Absence de contrôle des biens sensibles	ORG_04	BPE_MMG.2.1
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_DEP	23	Absence de politique de protection de l'information	ORG_15	BGC_MSS.3.1
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_DEP	23	Absence de politique de protection de l'information	ORG_15	BPS_PSI.1.5
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_DEP	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	CGS_CIR.1.3
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BOS_ISI.3.1
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.1.1
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.4.1
ORG_DEP	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.2
ORG_DEP	23	Absence de contrôle des biens sensibles	ORG_15	BCM_CLI.2.1
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BCM_CLI.1.2
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BSP_SPR.3.1
ORG_DEP	23	Procédures de gestion et d'application des habilitations trop lourde à exploiter	ORG_36	CGS_GDH.1.3
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.1
ORG_DEP	23	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_DEP	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.1.1
ORG_DEP	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.3.1
ORG_DEP	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.4.1
ORG_DEP	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.1.1
ORG_DEP	23	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.3.1
ORG_DEP	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.4.1
ORG_DEP	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.2
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_14	BOS_ISI.3.1
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_14	CGS_PAI.1.1
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.1.1
ORG_DEP	23	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.2.1
ORG_DEP	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.3.1
ORG_DEP	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.1
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_DEP	23	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.1.1
ORG_DEP	23	Absence de contrôle des biens sensibles	ORG_15	BMA_IMT.2.1
ORG_DEP	23	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.1.1
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	CGS_PAI.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	CGS_PAI.1.2
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.4.1
ORG_DEP	24	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_DEP	24	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BGC_MSS.3.1
ORG_DEP	24	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.2.1
ORG_DEP	24	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BPS_PSI.1.5
ORG_DEP	24	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	24	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1
ORG_DEP	24	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_DEP	24	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_DEP	24	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1
ORG_DEP	24	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2
ORG_DEP	24	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.1.1
ORG_DEP	24	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.1.2
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	FPT_PHP.3.1
ORG_DEP	26	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_SEM.3.2
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_SEM.3.1
ORG_DEP	26	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_DEP	26	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	26	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2
ORG_DEP	26	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_SEM.1.1
ORG_DEP	26	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BOS_SAT.1.2
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.1.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	FPT_PHP.2.3
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	FPT_PHP.1/2.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	CGS_PDI.1.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.3.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.4.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.5.1
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.2.1
ORG_DEP	27	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.1.1
ORG_DEP	27	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.1.2
ORG_DEP	27	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BCM_CLI.2.1
ORG_DEP	27	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BGC_MSS.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	27	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_15	BPS_PSI.1.5
ORG_DEP	27	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	29	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.3
ORG_DEP	29	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.2
ORG_DEP	29	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.1
ORG_DEP	29	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.2.1
ORG_DEP	29	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	BGC_PRS.1.1
ORG_DEP	29	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.1.2
ORG_DEP	30	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.1
ORG_DEP	30	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.2
ORG_DEP	30	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.1.2
ORG_DEP	30	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	BGC_PRS.1.1
ORG_DEP	30	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.3
ORG_DEP	30	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.2.1
ORG_DEP	31	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.3
ORG_DEP	31	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.2.1
ORG_DEP	31	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.1
ORG_DEP	31	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	BGC_PRS.1.1
ORG_DEP	31	Absence de règles imposant l'utilisation de normes	ORG_04	BCO_RPS.1.2
ORG_DEP	31	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)	ORG_09	CGI_GIS.3.2
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_38	CRI_MOF.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_ZOS.5.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_ZOS.4.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_ZOS.3.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_ZOS.2.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_ZOS.1.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_SEM.3.2
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_SEM.3.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BPE_SEM.1.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	BOS_SAT.1.2
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	FPT_PHP.3.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	FPT_PHP.2.3
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	FPT_PHP.1/2.1
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_27	CGS_PDI.1.1
ORG_DEP	33	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	CGS_PDI.1.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	FPT_PHP.1/2.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	FPT_PHP.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	33	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	33	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	FPT_PHP.2.3
ORG_DEP	33	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_DEP	33	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_ZOS.3.1
ORG_DEP	33	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_DEP	33	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BOS_SAT.1.2
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_ZOS.5.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_SEM.1.1
ORG_DEP	33	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_ZOS.4.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_SEM.3.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_SEM.3.2
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_ZOS.1.1
ORG_DEP	33	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_33	BPE_ZOS.2.1
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_38	CRI_MOF.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.1
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.2
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	BCM_RLC.1.1
ORG_DEP	34	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	34	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	34	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	BCO_CEL.3.1
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.4
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.3
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	35	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	35	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.3
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	BCO_CEL.3.1
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.2
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	BCM_RLC.1.1
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.4
ORG_DEP	35	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme	LOG_07	CGS_GLI.1.1
ORG_DEP	36	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BCM_CLI.1.2
ORG_DEP	36	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_38	CRI_MOF.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	36	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BPS_PSI.1.5
ORG_DEP	36	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BCM_CLI.2.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_PAI.1.3
ORG_DEP	36	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BCM_CLI.1.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.2
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_PAI.1.2
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	LOG_11	CGS_PPS.2.1
ORG_DEP	36	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BGC_MSS.3.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.8
ORG_DEP	36	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	36	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	36	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	BMA_GAU.2.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	BMA_GAU.4.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_PAI.1.1
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.2
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.1.1
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.2.1
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.4.1
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.4
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.5
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.1
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.3
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.6
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.7
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.9
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.8
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.7
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.6
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.5
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.3
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.9
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	BMA_GAU.1.1
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_15	CGS_GDH.1.4
ORG_DEP	37	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	37	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_DEP	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.1.1
ORG_DEP	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_41	BPS_PSI.1.3
ORG_DEP	37	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BCM_CLI.1.1
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BCM_CLI.1.2
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BCO_CEL.5.1
ORG_DEP	37	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BGC_MSS.3.1
ORG_DEP	37	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_DEP	37	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	37	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BPS_PSI.1.5
ORG_DEP	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.5.1
ORG_DEP	37	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_DEP	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.4.1
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme	ORG_15	BCM_CLI.2.1
ORG_DEP	37	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1
ORG_DEP	38	Absence d'un contrôle de l'organisme mère sur les processus critiques	ORG_38	BOS_ISI.4.1
ORG_DEP	38	Absence d'un contrôle de l'organisme mère sur les processus critiques	ORG_38	CGS_GPC.1.2
ORG_DEP	38	Absence d'un contrôle de l'organisme mère sur les processus critiques	ORG_38	CGS_GPC.1.1
ORG_DEP	38	Absence d'un contrôle de l'organisme mère sur les processus critiques	ORG_38	CRI_MOF.1.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	BMA_GAU.2.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	BMA_GAU.4.1
ORG_DEP	39	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	BMA_GAU.1.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.6
ORG_DEP	39	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_DEP	39	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.5
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_15	CGS_GDH.1.4
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_PAI.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	39	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.3
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	LOG_11	CGS_PPS.2.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.8
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.7
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_PAI.1.2
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_PAI.1.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.9
ORG_DEP	39	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	39	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme	ORG_14	CGS_GDH.1.2
ORG_DEP	39	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2
ORG_DEP	39	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_DEP	39	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.1
ORG_DEP	40	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1
ORG_DEP	40	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	40	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	40	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	40	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.2
ORG_DEP	40	Absence de procédure de contrôle	ORG_33	BDM_SSA.1.1
ORG_DEP	40	Absence de sensibilisation sur les risques de sanction	PER_08	BSP_RIS.5.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	40	Absence de sensibilisation sur les risques de sanction	ORG_37	BSP_RIS.5.1
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.4.1
ORG_DEP	40	Absence de procédure de contrôle	ORG_33	BDM_SSA.4.1
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.3
ORG_DEP	40	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.1
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.6
ORG_DEP	40	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.2
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.5
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.4
ORG_DEP	40	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.9
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.8
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.7
ORG_DEP	40	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2
ORG_DEP	40	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.2.1
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.1.1
ORG_DEP	40	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_DEP	41	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	CCS_SRI.1.1
ORG_DEP	41	Absence de politique globale de gestion et d'archivage des traces et autres éléments de preuves	ORG_39	BMA_SAS.1.1
ORG_DEP	41	Absence de politique globale de gestion et d'archivage des traces et autres éléments de preuves	ORG_39	BMA_SAS.2.1
ORG_DEP	41	Absence de politique globale de gestion et d'archivage des traces et autres éléments de preuves	ORG_39	BGC_INT.2.1
ORG_DEP	41	Absence de définition des responsabilités	ORG_14	BSP_SPR.4.1
ORG_DEP	41	Absence de définition des responsabilités	ORG_14	BSP_SPR.1.1
ORG_DEP	41	Absence de définition des responsabilités	ORG_14	BPS_PSI.1.3
ORG_DEP	41	Absence de définition des responsabilités	ORG_14	BOS_ISI.3.1
ORG_DEP	41	Absence de procédures disciplinaires	ORG_37	BSP_RIS.5.1
ORG_DEP	41	Absence de procédures disciplinaires	ORG_37	BSP_RIS.5.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_DEP	41	Absence de politique globale de gestion et d'archivage des traces et autres éléments de preuves	ORG_39	BMA_SAS.3.1
ORG_DEP	41	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.1.1
ORG_DEP	41	Présence d'enjeu politico-économique fort	ORG_31	CEI_ABS.1.6
ORG_DEP	41	Présence d'enjeu politico-économique fort	ORG_31	CEI_ABS.1.7
ORG_DEP	41	Changement de politique ou de stratégie d'organisation	ORG_33	CGS_OES.1.3
ORG_DEP	41	Changement de politique ou de stratégie d'organisation	ORG_33	CGS_OES.1.2
ORG_DEP	41	Changement de politique ou de stratégie d'organisation	ORG_33	BMA_MAS.3.1
ORG_DEP	41	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur	ORG_14	BSP_SPR.4.1
ORG_DEP	42	Présence d'un conflit politico-économique entre le pays d'appartenance de l'organisation et le pays accueillant l'organisation	ORG_31	CRH_PDP.1.1

4.6.2 ORG_GEN : Organisation de l'organisme

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)	ORG_14	CGI_LCI.1.6
ORG_GEN	1	Absence de suivi des contrats de maintenance des équipements de protection incendie	ORG_27	BPE_SEM.4.1
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)	ORG_14	CGI_LCI.1.4
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)	ORG_24	CGI_LCI.1.3
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)	ORG_24	CGI_LCI.1.2
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.3.1
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.3.2
ORG_GEN	1	Absence de gestion des procès verbaux de contrôle des équipements de secours	ORG_27	CET_EIP.1.6
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.1
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.2
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)	ORG_14	CGI_LCI.1.7
ORG_GEN	1	Absence de suivi des contrats de maintenance des équipements de protection incendie	ORG_27	CGS_GMA.1.2
ORG_GEN	1	Absence de gestion des procès verbaux de contrôle des équipements de secours	ORG_27	BGC_INT.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)	ORG_24	CGI_LCI.1.1
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.4
ORG_GEN	1	Absence de suivi des contrats de maintenance des équipements de protection incendie	ORG_27	CGS_GMA.3.3
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)	ORG_14	CGI_LCI.1.5
ORG_GEN	1	Absence de suivi des contrats de maintenance des équipements de protection incendie	ORG_27	CGS_GMA.3.2
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.3
ORG_GEN	1	Absence de suivi des contrats de maintenance des équipements de protection incendie	ORG_27	CGS_GMA.3.1
ORG_GEN	1	Absence de suivi des contrats de maintenance des équipements de protection incendie	ORG_27	CGS_GMA.1.1
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.2.1
ORG_GEN	2	Absence de garantie de bon fonctionnement des détecteurs de présence d'eau	ORG_27	CGS_GMA.1.2
ORG_GEN	2	Absence de consignes d'alerte, de réaction, d'information en cas de dégât des eaux (absence d'identification des vanne d'arrêts…)	ORG_24	CCS_SIN.3.4
ORG_GEN	2	Absence de garantie de bon fonctionnement des détecteurs de présence d'eau	ORG_27	BPE_SEM.4.1
ORG_GEN	2	Absence de gestion des procès verbaux de contrôle des équipements de secours	ORG_27	BGC_INT.2.1
ORG_GEN	2	Absence de garantie de bon fonctionnement des détecteurs de présence d'eau	ORG_27	CGS_GMA.1.1
ORG_GEN	2	Absence de consignes d'alerte, de réaction, d'information en cas de dégât des eaux (absence d'identification des vannes d'arrêts…)	ORG_24	CCS_SIN.3.2
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.2.1
ORG_GEN	2	Absence de gestion des procès verbaux de contrôle des équipements de secours	ORG_27	CET_EIP.1.6
ORG_GEN	2	Absence de consignes d'alerte, de réaction, d'information en cas de dégât des eaux (absence d'identification des vannes d'arrêts…)	ORG_24	CCS_SIN.3.5
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.4
ORG_GEN	2	Absence de consignes d'alerte, de réaction, d'information en cas de dégât des eaux (absence d'identification des vannes d'arrêts…)	ORG_24	CCS_SIN.2.1
ORG_GEN	2	Absence de consignes d'alerte, de réaction, d'information en cas de dégât des eaux (absence d'identification des vannes d'arrêts…)	ORG_24	CCS_SIN.2.3
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.3.1
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.3.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	2	Absence de consignes d'alerte, de réaction, d'information en cas de dégât des eaux (absence d'identification des vannes d'arrêts…)	ORG_24	CCS_SIN.3.1
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.1
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.3
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.2
ORG_GEN	3	Absence de suivi des contrats de maintenance	ORG_27	CGS_GMA.3.1
ORG_GEN	3	Absence de suivi des contrats de maintenance	ORG_27	CGS_GMA.1.2
ORG_GEN	3	Absence de suivi des contrats de maintenance	ORG_27	CGS_GMA.1.1
ORG_GEN	3	Absence de mesures en cas d'interruption du service de climatisation	ORG_16	CCS_SIN.3.4
ORG_GEN	3	Absence de suivi des contrats de maintenance	ORG_27	BPE_SEM.4.1
ORG_GEN	3	Absence de mesures en cas d'interruption du service de climatisation	ORG_16	CCS_SIN.3.5
ORG_GEN	3	Absence de mesures en cas d'interruption du service de climatisation	ORG_16	CCS_SIN.2.3
ORG_GEN	3	Absence de mesures en cas d'interruption du service de climatisation	ORG_16	CCS_SIN.3.1
ORG_GEN	3	Absence de mesures en cas d'interruption du service de climatisation	ORG_16	CCS_SIN.3.2
ORG_GEN	3	Absence de suivi des contrats de maintenance	ORG_27	CGS_GMA.3.2
ORG_GEN	3	Absence de suivi des contrats de maintenance	ORG_27	CGS_GMA.3.3
ORG_GEN	3	Absence de mesures en cas d'interruption du service de climatisation	ORG_16	CCS_SIN.2.1
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.4
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.6
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.1
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.3
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.4
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.2.1
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.3.1
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.3.2
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.3
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.4
ORG_GEN	4	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.2
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.5
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.4
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.5
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.4.1
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.2
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence	ORG_17	CCS_SIN.1.2
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.3
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.4.5
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.1
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.2
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.6
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.1
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.2
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.1.1
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.3
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.6
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.1
ORG_GEN	4	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.2.2
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.2
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.3
ORG_GEN	4	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.1
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	BGC_PRE.1.1
ORG_GEN	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.4
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	BPE_SEM.1.1
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.7
ORG_GEN	5	Absence de couverture d'assurance en cas de destruction de matériel	ORG_44	CRR_ETU.1.2
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.5
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.3
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.2
ORG_GEN	5	Absence de couverture d'assurance en cas de destruction de matériel	ORG_44	CRR_ETU.2.2
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	BPE_SEM.5.1
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.6
ORG_GEN	5	Absence de couverture d'assurance en cas de destruction de matériel	ORG_44	CRR_ETU.1.1
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_GEN	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_GEN	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_GEN	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_GEN	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_GEN	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_GEN	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_GEN	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_GEN	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_GEN	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_GEN	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_GEN	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_GEN	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_GEN	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_GEN	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_GEN	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_GEN	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_GEN	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_GEN	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_GEN	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_GEN	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_GEN	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_GEN	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_GEN	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_GEN	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_GEN	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_GEN	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_GEN	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_GEN	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.7
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.6
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.5
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.2
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.3
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.1
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.4
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.7
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.3
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.5
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.6
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.1
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.4
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.2
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.7
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.6
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.5
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.4
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.3
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.2
ORG_GEN	17	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	17	Absence de politique de protection de l'information	ORG_15	BPS_PSI.1.5
ORG_GEN	17	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	17	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	17	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.1
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	17	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	17	Absence de politique de protection de l'information	ORG_15	BCM_CLI.2.1
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	17	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	17	Absence de politique de protection de l'information	ORG_15	BGC_MSS.3.1
ORG_GEN	17	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.2
ORG_GEN	18	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.4.1
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.1.1
ORG_GEN	18	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	18	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.7
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.5
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.3
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.2
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.1
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	18	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.2.1
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	18	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_15	CGS_GDH.1.4
ORG_GEN	18	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	19	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	19	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.1
ORG_GEN	19	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.1.1
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.5
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.7
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.2.1
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.4.1
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_15	CGS_GDH.1.4
ORG_GEN	19	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	19	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	19	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.2
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.3
ORG_GEN	20	Absence de contrôle des biens sensibles	ORG_15	BMA_IMT.2.1
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité	ORG_21	CGI_GIS.2.5
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité	ORG_21	CGI_GIS.2.4
ORG_GEN	20	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.1.1
ORG_GEN	20	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	20	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	20	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	20	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité	ORG_21	CGI_GIS.2.3
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	20	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.1.1
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	20	Absence de contrôle des biens sensibles	ORG_15	BCM_CLI.2.1
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	20	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.2.1
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	20	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BCM_CLI.1.2
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	CGS_CIR.1.3
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité	ORG_21	CGI_GIS.2.2
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BOS_ISI.3.1
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.2
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BSP_SPR.3.1
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.4.1
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.1.1
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité	ORG_21	BSP_RIS.1.1
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité	ORG_21	CGI_GIS.2.1
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité	ORG_21	BSP_RIS.4.1
ORG_GEN	20	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	20	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.1
ORG_GEN	21	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	21	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	21	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	21	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	21	Absence de règles de contrôle des entrées/sorties des matériels dans l'organisme	ORG_02	CET_EGT.1.9
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol	ORG_21	BSP_RIS.4.1
ORG_GEN	21	Absence de règles de contrôle des entrées/sorties des matériels dans l'organisme	ORG_02	CET_EGT.1.10
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol	ORG_21	CGI_GIS.2.2
ORG_GEN	21	Absence de règles de contrôle des entrées/sorties des matériels dans l'organisme	ORG_02	CET_EGT.1.8
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol	ORG_21	CGI_GIS.2.5
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol	ORG_21	CGI_GIS.2.3
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol	ORG_21	CGI_GIS.2.1
ORG_GEN	21	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol	ORG_21	BSP_RIS.1.1
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol	ORG_21	CGI_GIS.2.4
ORG_GEN	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	FDP_RIP.1.1
ORG_GEN	22	Absence de contrôle des biens sensibles	ORG_04	BCM_RLC.1.1
ORG_GEN	22	Absence de contrôle des biens sensibles	ORG_04	BPE_MMG.2.1
ORG_GEN	22	Absence de contrôle des biens sensibles	ORG_04	BMA_IMT.2.1
ORG_GEN	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	FDP_RIP.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	BPE_SEM.6.1
ORG_GEN	22	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	BGC_MSS.2.1
ORG_GEN	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.1
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.4.1
ORG_GEN	23	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.2.1
ORG_GEN	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.2
ORG_GEN	23	Absence de politique de protection de l'information	ORG_15	BGC_MSS.3.1
ORG_GEN	23	Absence de politique de protection de l'information	ORG_15	BPS_PSI.1.5
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	23	Absence de contrôle des biens sensibles	ORG_15	BMA_IMT.2.1
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	23	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.3.1
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	CGS_CIR.1.3
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BOS_ISI.3.1
ORG_GEN	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.2.1
ORG_GEN	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_14	CGS_PAI.1.1
ORG_GEN	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.1.1
ORG_GEN	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.3.1
ORG_GEN	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.4.1
ORG_GEN	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.1.1
ORG_GEN	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.3.1
ORG_GEN	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.4.1
ORG_GEN	23	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_14	BOS_ISI.3.1
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.1
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.1.1
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.4.1
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	CGS_PAI.1.2
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	CGS_PAI.1.3
ORG_GEN	23	Absence de contrôle des biens sensibles	ORG_15	BCM_CLI.2.1
ORG_GEN	23	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.1.1
ORG_GEN	23	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.2
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BCM_CLI.1.2
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BSP_SPR.3.1
ORG_GEN	23	Procédures de gestion et d'application des habilitations trop lourde à exploiter	ORG_36	CGS_GDH.1.3
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.1.1
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_MAS.2.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.3
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.2
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.2.3
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.4.1
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BGC_EIL.1.1
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_GAU.2.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.2
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_MAS.3.1
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_SAS.2.1
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BSP_FOU.1.1
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BPS_PSI.1.3
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BDM_SSA.3.1
ORG_GEN	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	BSP_SPR.3.1
ORG_GEN	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	BOS_SAT.1.5
ORG_GEN	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	CET_PLD.1.2
ORG_GEN	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	CET_EGT.1.3
ORG_GEN	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.1
ORG_GEN	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.2
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.1.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.3.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BGC_INT.2.1
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.3
ORG_GEN	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	FPT_PHP.2.3
ORG_GEN	25	Absence de contrôle des biens sensibles	ORG_04	BPE_MMG.2.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_38	CRI_MOF.1.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_SEM.3.2
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_SEM.3.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_SEM.1.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	FPT_PHP.3.1
ORG_GEN	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	CGS_PDI.1.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.5.1
ORG_GEN	25	Absence de contrôle des biens sensibles	ORG_04	BPE_MMG.1.1
ORG_GEN	25	Absence de contrôle des biens sensibles	ORG_04	BMA_IMT.2.1
ORG_GEN	25	Absence de contrôle des biens sensibles	ORG_04	BGC_MSS.3.1
ORG_GEN	25	Absence de contrôle des biens sensibles	ORG_04	BGC_MSS.1.1
ORG_GEN	25	Absence de contrôle des biens sensibles	ORG_04	BCM_CLI.2.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BOS_SAT.1.2
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	FPT_PHP.1/2.1
ORG_GEN	25	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	CGS_OML.1.1
ORG_GEN	25	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.3
ORG_GEN	25	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.4
ORG_GEN	25	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.3
ORG_GEN	25	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.2
ORG_GEN	25	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.6.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.2.1
ORG_GEN	25	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.2
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.4.1
ORG_GEN	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	BOS_SAT.1.3
ORG_GEN	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	BDM_SED.4.1
ORG_GEN	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	BDM_ESS.1.1
ORG_GEN	25	Absence de procédures de qualification opérationnelle	ORG_26	BDM_SED.4.1
ORG_GEN	25	Absence de procédures de qualification opérationnelle	ORG_26	BDM_ESS.1.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.1.1
ORG_GEN	25	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique	ORG_34	BOS_ISI.5.3
ORG_GEN	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	25	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme	ORG_04	BPE_ZOS.3.1
ORG_GEN	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_04	CPS_PPT.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	26	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.3.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.4.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.1.1
ORG_GEN	26	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	26	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.2.1
ORG_GEN	26	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.3.1
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_04	CPS_PPT.1.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.1
ORG_GEN	26	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.1.1
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_04	CPS_PPT.1.4
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_04	BGC_EIL.5.1
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_06	BGC_EIL.5.1
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_04	CPS_PPT.1.5
ORG_GEN	26	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.1.1
ORG_GEN	26	Absence de contrôle des biens sensibles	ORG_15	BCM_CLI.2.1
ORG_GEN	26	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_04	CPS_PPT.1.2
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.2
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.3
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.2
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_06	CPS_PPT.1.5
ORG_GEN	26	Absence de contrôle des biens sensibles	ORG_15	BMA_IMT.2.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.3.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BGC_INT.2.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.2.3
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_06	CPS_PPT.1.4
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_06	CPS_PPT.1.3
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_06	CPS_PPT.1.2
ORG_GEN	26	Absence de politique globale de lutte contre le code malveillant	ORG_06	BGC_PLM.1.1
ORG_GEN	26	Absence de politique de protection des postes de travail	ORG_06	CPS_PPT.1.1
ORG_GEN	26	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.2
ORG_GEN	26	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.2.1
ORG_GEN	27	Absence de règles de protection en confidentialité des informations, exploitables pour localiser un personnel (demandes de billets, registre d'entrée/sortie…)	ORG_15	CPD_DGL.1.1
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	BPE_SEM.4.1
ORG_GEN	28	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements	ORG_09	BGC_PRS.1.1
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.3
ORG_GEN	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	BSP_RIS.4.1
ORG_GEN	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_GEN	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.6
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.2
ORG_GEN	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.5
ORG_GEN	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.1
ORG_GEN	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	PHY_08	CCS_CSG.1.2
ORG_GEN	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.1.1
ORG_GEN	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_GEN	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.7
ORG_GEN	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_GEN	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_GEN	28	Absence de consignes de réaction rapide pour la protection des matériels en cas de dégât des eaux ou d'incendie	ORG_24	CCS_SIN.2.3
ORG_GEN	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.3.3
ORG_GEN	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	BPE_SEM.4.1
ORG_GEN	28	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements	ORG_09	CEI_ABS.1.5
ORG_GEN	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.1
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.2
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.1
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.2
ORG_GEN	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	BOS_ISI.1.2
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.1
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.3
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.1.2
ORG_GEN	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.3.1
ORG_GEN	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.3.2
ORG_GEN	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	CGI_GIS.3.3
ORG_GEN	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	CGI_GIS.3.2
ORG_GEN	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	CGI_GIS.3.1
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.2
ORG_GEN	29	Absence de reporting sur les dysfonctionnements	ORG_21	CGI_GIS.3.2
ORG_GEN	29	Absence de reporting sur les dysfonctionnements	ORG_21	CGI_GIS.3.3
ORG_GEN	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)	ORG_04	BPE_SEM.1.1
ORG_GEN	29	Absence de reporting sur les dysfonctionnements	ORG_21	BOS_ISI.1.2
ORG_GEN	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)	PHY_10	CIS_ADL.2.1
ORG_GEN	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)	ORG_04	CCS_CSG.1.4
ORG_GEN	29	Absence de reporting sur les dysfonctionnements	ORG_21	BSP_RIS.4.1
ORG_GEN	29	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements	ORG_09	CEI_ABS.1.5
ORG_GEN	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_GEN	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_GEN	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_GEN	29	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements	ORG_09	BGC_PRS.1.1
ORG_GEN	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_GEN	29	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.3
ORG_GEN	29	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.4
ORG_GEN	29	Absence de procédures de qualification opérationnelle	ORG_26	BDM_ESS.1.1
ORG_GEN	29	Absence de procédures de qualification opérationnelle	ORG_26	BDM_SED.4.1
ORG_GEN	29	Absence de reporting sur les dysfonctionnements	ORG_21	CGI_GIS.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BCA_AGC.1.1
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.3
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.5
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BGC_PRE.3.1
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.7
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.8
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BCA_AGC.3.1
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	CGI_GIS.3.2
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	CGI_GIS.3.3
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.2
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.4
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BGC_PRS.1.1
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	CGI_GIS.3.1
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BCA_AGC.5.1
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.2.1
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.1.1
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.6

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	30	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements conduisant à la saturation des espaces de stockage ou des ressources de traitement	ORG_09	CCS_CSG.1.2
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.1
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.6
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application	ORG_33	BMA_MAR.6.1
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.4
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.3
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.2
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.1
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application	ORG_33	BMA_MAR.1.1
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.7
ORG_GEN	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.5
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.3
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application	ORG_33	BMA_MAR.7.1
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.2
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.1
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.4

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application	ORG_33	BMA_MAA.2.1
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application	ORG_33	BMA_EMA.1.1
ORG_GEN	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_GEN	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_GEN	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.5
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.6
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.7
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.8
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BGC_PRE.3.1
ORG_GEN	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.2.1
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.1.1
ORG_GEN	31	Absence d'homogénéité du parc informatique	ORG_42	BDM_ESS.1.1
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application	ORG_33	BMA_MAA.1.1
ORG_GEN	31	Absence d'homogénéité du parc informatique	ORG_42	BGC_PRS.2.1
ORG_GEN	31	Absence d'homogénéité du parc informatique	ORG_42	CGS_REC.1.1
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application	ORG_33	BGC_PRE.4.1
ORG_GEN	31	Absence d'homogénéité du parc informatique	ORG_42	BDM_SFS.1.1
ORG_GEN	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	BGC_PRE.2.1
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.2
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.1
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.3
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BMA_MAR.5.1
ORG_GEN	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	CDO_SDC.1.1
ORG_GEN	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	BGC_PRE.2.2
ORG_GEN	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	BCM_RLC.1.1
ORG_GEN	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	BCO_RPS.2.1
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.1
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	BPE_SEM.4.1
ORG_GEN	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.3
ORG_GEN	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.1
ORG_GEN	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.2
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.2
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.3
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.2.1
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.5
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.4
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.2
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.3
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.2
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.1
ORG_GEN	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.4
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BGC_PRE.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	32	Absence de plan de formation à la maintenance des nouveaux systèmes	ORG_14	CGS_GMA.2.1
ORG_GEN	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.6
ORG_GEN	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.5
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.1
ORG_GEN	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	CPS_DEV.1.2
ORG_GEN	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	CPS_DEV.1.1
ORG_GEN	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	BDM_SED.5.1
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	CGS_GMA.4.1
ORG_GEN	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_GEN	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BCM_RLC.1.1
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.1.1
ORG_GEN	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.8
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.7
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.6
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.5
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.4
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.3
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.2
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.1
ORG_GEN	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_GEN	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.1
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BGC_MSS.4.1
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.2.1
ORG_GEN	33	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	33	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_MAS.1.1
ORG_GEN	33	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_REU.2.1
ORG_GEN	33	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAS.2.1
ORG_GEN	33	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAR.1.1
ORG_GEN	33	Absence de procédure de contrôle	ORG_33	BDM_SSA.4.1
ORG_GEN	33	Absence de sensibilisation sur les risques de sanction	ORG_37	BSP_RIS.5.1
ORG_GEN	33	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.2
ORG_GEN	33	Absence de charte informatique précisant les exigences d'utilisation	ORG_04	CCS_CHI.1.1
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.4
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.1
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.2
ORG_GEN	33	Absence de procédure de contrôle	ORG_33	BDM_SSA.1.1
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.3
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.5
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.6
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.7
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	33	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	33	Absence de sensibilisation sur les risques de sanction	PER_08	BSP_RIS.5.2
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	34	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_41	BSP_FOU.1.1
ORG_GEN	34	Absence de procédure de contrôle	ORG_33	BDM_SSA.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.1.1
ORG_GEN	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BPS_PSI.1.3
ORG_GEN	34	Absence de charte informatique précisant les exigences d'utilisation	ORG_04	CCS_CHI.1.1
ORG_GEN	34	Absence de procédure de contrôle	ORG_33	BDM_SSA.1.1
ORG_GEN	34	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.2
ORG_GEN	34	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.1
ORG_GEN	34	Absence de sensibilisation sur les risques de sanction	ORG_37	BSP_RIS.5.1
ORG_GEN	34	Absence de sensibilisation sur les risques de sanction	PER_08	BSP_RIS.5.2
ORG_GEN	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.2.1
ORG_GEN	35	La politique de sécurité ne traite pas du rappel des obligations et des responsabilités de chacun en matière civile, pénale et réglementaire	ORG_40	BCO_CEL.1.1
ORG_GEN	35	La politique de sécurité ne traite pas du rappel des obligations et des responsabilités de chacun en matière civile, pénale et réglementaire	ORG_41	BSP_FOU.1.1
ORG_GEN	35	La politique de sécurité ne traite pas du rappel des obligations et des responsabilités de chacun en matière civile, pénale et réglementaire	ORG_40	BPS_PSI.1.3
ORG_GEN	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_41	BSP_FOU.1.1
ORG_GEN	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.2.1
ORG_GEN	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BPS_PSI.1.3
ORG_GEN	35	Absence de charte informatique précisant les exigences d'utilisation	ORG_04	CCS_CHI.1.1
ORG_GEN	35	Absence de contrôle de l'origine des produits	ORG_20	CGS_OML.1.1
ORG_GEN	35	Absence de contrôle de certification des produits	ORG_20	CGS_OML.1.2
ORG_GEN	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.1.1
ORG_GEN	36	Absence de contrôle d'accès à l'information	ORG_15	BMA_MAA.1.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.7.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.4.1
ORG_GEN	36	Absence de contrôle d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_GEN	36	Absence de contrôle d'accès à l'information	ORG_30	BMA_MAR.7.1
ORG_GEN	36	Absence de contrôle d'accès à l'information	ORG_30	BMA_MAS.2.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.3.1
ORG_GEN	36	Absence de contrôle d'accès à l'information	ORG_15	CGS_GDH.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAS.2.1
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.5
ORG_GEN	36	Absence de contrôle d'accès à l'information	ORG_30	BMA_MAS.3.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_SAS.1.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_SAS.2.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BOS_SAT.1.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.2.1
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.7
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.6
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.3
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.2
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.1
ORG_GEN	36	Absence de charte informatique précisant les exigences d'utilisation	ORG_04	CCS_CHI.1.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_SEM.1.1
ORG_GEN	36	Absence de procédures de contrôle des disquettes extérieures	ORG_06	BGC_PLM.1.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.1
ORG_GEN	36	Absence de prévention et la détection des virus et d'autres logiciels malveillants	ORG_06	BGC_PLM.1.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.6
ORG_GEN	36	Absence de procédures de contrôle des disquettes extérieures	ORG_06	BGC_MSS.1.1
ORG_GEN	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.1
ORG_GEN	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.2
ORG_GEN	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.4
ORG_GEN	36	Absence de plan de formation sur les problèmes de sécurité	PER_02	CFO_SPS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	36	Absence de politique des habilitations d'accès à l'information	ORG_30	BMA_GAU.1.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.2
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.3
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.5
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.1.1
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.4
ORG_GEN	36	Absence de politique des habilitations d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.4
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_EMA.1.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BGC_GER.1.1
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	CEI_ABS.1.1
ORG_GEN	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.7
ORG_GEN	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_GEN	36	Absence de plan de formation sur les problèmes de sécurité	PER_02	CRR_SEN.1.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.4.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.2.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	BMA_GAU.1.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.9
ORG_GEN	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels	ORG_30	CGS_GDH.1.8
ORG_GEN	36	Absence de plan de formation sur les problèmes de sécurité	PER_02	BSP_FOU.1.1
ORG_GEN	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_14	CGS_PAI.1.1
ORG_GEN	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_14	BCM_CLI.1.2
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles	PER_05	BSP_SPR.1.1
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BPS_PSI.1.4
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles	PER_05	BSP_SPR.3.1
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles	PER_05	BSP_SPR.4.1
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles	ORG_14	BSP_SPR.1.1
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles	ORG_14	BSP_SPR.3.1
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles	ORG_14	BSP_SPR.4.1
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles	ORG_14	BSP_FOU.1.1
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BCO_RPS.1.1
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BCO_RPS.2.1
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BSP_RIS.5.1
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BCO_RPS.1.2
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.1.1
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.7
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BSP_RIS.5.2
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.1
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.2
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.3
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.4
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.6

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_30	BMA_MAS.2.1
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BGC_PRE.3.1
ORG_GEN	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_14	CGS_CIR.1.3
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.2.1
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_15	CGS_GDH.1.1
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_15	BMA_MAA.1.1
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_30	BMA_MAR.7.1
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_30	BMA_MAS.3.1
ORG_GEN	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_15	BCO_CEL.4.1
ORG_GEN	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_15	CGS_CIR.1.1
ORG_GEN	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_15	CGS_CIR.1.2
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.8
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BSP_SPR.4.1
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_30	BGC_PRE.4.1
ORG_GEN	37	Absence de contrôle d'accès à l'information	ORG_30	BCO_CEL.5.1
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BCO_CEL.4.1
ORG_GEN	37	Manque d'informations sur les lois et les règlements appliquées au traitement de l'information	ORG_41	BPS_PSI.1.3
ORG_GEN	37	Manque d'informations sur les lois et les règlements appliquées au traitement de l'information	ORG_40	BCO_CEL.1.1
ORG_GEN	37	Manque d'informations sur les lois et les règlements appliquées au traitement de l'information	ORG_40	BCO_CEL.4.1
ORG_GEN	37	Manque d'informations sur les lois et les règlements appliquées au traitement de l'information	ORG_40	BCO_CEL.5.1
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.5
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives	ORG_18	BSP_SPR.1.1
ORG_GEN	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.1
ORG_GEN	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.4
ORG_GEN	38	Absence de formation sur les matériels ou logiciels utilisés	PER_12	BSP_FOU.2.1
ORG_GEN	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.2
ORG_GEN	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.3
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BDM_SSA.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BDM_SSA.4.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_MAS.3.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.1.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.2.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.3.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BOS_SAT.1.3
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BOS_SAT.2.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	PER_08	BSP_RIS.5.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.7.2
ORG_GEN	39	Les attributions des utilisateurs ne sont pas clairement définies	ORG_14	CGS_GDH.2.2
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	PER_08	BMA_MAS.6.1
ORG_GEN	39	Les attributions des utilisateurs ne sont pas clairement définies	ORG_14	CGS_GDH.2.1
ORG_GEN	39	Absence de définition du droit d'en connaître	ORG_33	CGS_PAI.2.2
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	PER_08	BSP_RIS.5.2
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.7.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.4.1
ORG_GEN	39	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.1.1
ORG_GEN	39	Absence d'un règlement définissant les droits	ORG_33	CGS_PAI.2.1
ORG_GEN	39	Absence d'un règlement définissant les droits	ORG_33	CGS_PAI.2.3
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.2.1
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.4.1
ORG_GEN	40	Organisation inadaptée	ORG_14	CGS_OES.1.1
ORG_GEN	40	Absence de procédure de remontée d'information en cas de détection	ORG_24	BSP_RIS.1.1
ORG_GEN	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_REU.2.1
ORG_GEN	40	Absence de procédure de remontée d'information en cas de détection	ORG_24	BSP_RIS.2.1
ORG_GEN	40	Absence de procédure de contrôle	ORG_33	BDM_SSA.1.1
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_GEN	40	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.2
ORG_GEN	40	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.1
ORG_GEN	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAR.1.1
ORG_GEN	40	Absence de procédure de contrôle	ORG_33	BDM_SSA.4.1
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_GEN	40	Absence de procédure d'habilitation du personnel	ORG_30	BMA_GAU.2.1
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_GEN	40	Absence de procédure d'habilitation du personnel	ORG_30	BMA_GAU.1.1
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.2
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.3
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.5
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	CGS_GDH.1.7
ORG_GEN	40	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_GEN	40	Absence de communication et d'information des procédures d'habilitation au personnel	ORG_41	BMA_GAU.1.1
ORG_GEN	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.4
ORG_GEN	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.2
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées	ORG_14	BMA_GAU.1.1
ORG_GEN	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAS.2.1
ORG_GEN	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.1
ORG_GEN	40	Absence de procédure d'habilitation du personnel	LOG_11	CGS_PPS.2.1
ORG_GEN	40	Absence de communication et d'information des procédures d'habilitation au personnel	ORG_41	BSP_FOU.1.1
ORG_GEN	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_MAS.1.1
ORG_GEN	40	Absence de communication et d'information des procédures d'habilitation au personnel	ORG_41	BGC_PRE.1.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.2.3
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BMA_SAS.3.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BMA_SAS.2.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.3.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BMA_SAS.1.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.3.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.2.3
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.1/2.2
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.3.2
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.1/2.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.4.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.2.2
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BGC_INT.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.3.3
ORG_GEN	41	Changement de politique ou de stratégie d'organisation	ORG_33	CGS_OES.1.3
ORG_GEN	41	Absence de définition des responsabilités	ORG_14	BOS_ISI.3.1
ORG_GEN	41	Absence de définition des responsabilités	ORG_14	BPS_PSI.1.3
ORG_GEN	41	Absence de définition des responsabilités	ORG_14	BSP_SPR.1.1
ORG_GEN	41	Absence de procédures disciplinaires	ORG_37	BSP_RIS.5.1
ORG_GEN	41	Absence de procédures disciplinaires	ORG_37	BSP_RIS.5.2
ORG_GEN	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAR.1.1
ORG_GEN	41	Absence de définition des responsabilités	ORG_14	BSP_SPR.4.1
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.2.1
ORG_GEN	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_REU.2.1
ORG_GEN	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAS.2.1
ORG_GEN	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_MAS.1.1
ORG_GEN	41	Changement de politique ou de stratégie d'organisation	ORG_33	BMA_MAS.3.1
ORG_GEN	41	Changement de politique ou de stratégie d'organisation	ORG_33	CGS_OES.1.2
ORG_GEN	42	Présence d'un conflit politico-économique entre le pays d'appartenance de l'organisation et le pays accueillant l'organisation	ORG_31	CRH_PDP.1.1
ORG_GEN	42	Présence d'une épidémie virale locale	PER_04	CFO_FRS.1.4
ORG_GEN	42	Présence d'une épidémie virale locale	PER_04	CFO_FRS.1.1
ORG_GEN	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.3
ORG_GEN	42	Présence d'une épidémie virale locale	PER_04	CFO_FRS.1.3
ORG_GEN	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.1
ORG_GEN	42	Présence d'une épidémie virale locale	PER_04	CFO_FRS.1.5
ORG_GEN	42	Présence d'une épidémie virale locale	PER_04	CRH_DDE.1.1
ORG_GEN	42	Présence d'une épidémie virale locale	PER_04	CRH_DDE.1.2
ORG_GEN	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.4.1
ORG_GEN	42	Présence d'une épidémie virale locale	PER_04	CFO_FRS.1.2
ORG_GEN	42	Absence de processus de gestion de la continuité des activités professionnelles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_GEN	42	Absence de processus de gestion de la continuité des activités professionnelles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_GEN	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.5.1
ORG_GEN	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	PER_10	BSP_FOU.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_GEN	42	Absence de processus de gestion de la continuité des activités professionnelles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_GEN	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.3.1
ORG_GEN	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.4
ORG_GEN	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.2
ORG_GEN	42	Absence de processus de gestion de la continuité des activités professionnelles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_GEN	42	Absence d'équipe de protection du personnel	ORG_45	CRH_PDP.1.1
ORG_GEN	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.1.1
ORG_GEN	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.2.1
ORG_GEN	42	Absence de processus de gestion de la continuité des activités professionnelles de l'organisme	ORG_16	BCA_AGC.3.1

4.6.3 ORG_PRO : Organisation de projet ou d'un système

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.1
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.2
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.3
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.2
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.3
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.4
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.3
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.5
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.3
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.5
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.6
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.4.5
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.1
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.2
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.4
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.4
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.1
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.1.1
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.6
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.4
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.4.1
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.6
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.1
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	BGC_PRE.1.1
ORG_PRO	1	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.5
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.1
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.4.1
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.1.1
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.4.5
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.3
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.1
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.1
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.6
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.4
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.4
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.2
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.6
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.2
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.3
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.5
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.4
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.3
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.2
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.3
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.4
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.6
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	BGC_PRE.1.1
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.2
ORG_PRO	2	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.1
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.2
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.3
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.6
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	BGC_PRE.1.1
ORG_PRO	4	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.2
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.3
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.3
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.4
ORG_PRO	4	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.1.1
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.3
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.5
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.2.5
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.3.6
ORG_PRO	4	Absence de couverture d'assurance en cas de sinistre grave	ORG_44	CRR_ETU.2.2
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	CGI_GDC.4.5
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.4
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.1.1
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_14	BSP_SPR.4.1
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.4.1
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.2
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.4

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.4
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.2
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.1
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.3.1
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.6
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.2.2
ORG_PRO	4	Absence d'organisation de gestion de crise	ORG_24	CGI_GDC.1.1
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.2
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.7
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.6
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.3
ORG_PRO	5	Absence de couverture d'assurance en cas de destruction de matériel	ORG_44	CRR_ETU.2.2
ORG_PRO	5	Absence de couverture d'assurance en cas de destruction de matériel	ORG_44	CRR_ETU.1.1
ORG_PRO	5	Absence de couverture d'assurance en cas de destruction de matériel	ORG_44	CRR_ETU.1.2
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.1
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	BPE_SEM.5.1
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	BPE_SEM.1.1
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)	ORG_04	CCS_CSG.1.5
ORG_PRO	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_PRO	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_PRO	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_PRO	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_PRO	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_PRO	6	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_PRO	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_PRO	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_PRO	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_PRO	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_PRO	7	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_PRO	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_PRO	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_PRO	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_PRO	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_PRO	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_PRO	8	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_PRO	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_PRO	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_PRO	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_PRO	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_PRO	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_PRO	9	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_PRO	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.1
ORG_PRO	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.4
ORG_PRO	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.2
ORG_PRO	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.1
ORG_PRO	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.3.5
ORG_PRO	10	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SIN.2.3
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.7
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.1
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.3
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.4
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.5
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.6
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.6
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.1
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.2
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.4
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.7
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.3
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.5
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.2
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.3
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.5
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.6
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.4
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.7
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)	ORG_24	CCS_SSE.1.1
ORG_PRO	18	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.2
ORG_PRO	18	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.1
ORG_PRO	18	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.2
ORG_PRO	18	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.3
ORG_PRO	18	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.4
ORG_PRO	18	Absence de politique de protection de l'information	ORG_15	BPS_PSI.1.5
ORG_PRO	18	Absence de politique de protection de l'information	ORG_15	BGC_MSS.3.1
ORG_PRO	18	Absence de politique de protection de l'information	ORG_15	BCM_CLI.2.1
ORG_PRO	18	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	18	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.4
ORG_PRO	18	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_PRO	18	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.1
ORG_PRO	19	Absence de politique de protection de l'information	ORG_15	BPS_PSI.1.5
ORG_PRO	19	Absence de politique de protection de l'information	ORG_15	BCM_CLI.2.1
ORG_PRO	19	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.2
ORG_PRO	19	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.1
ORG_PRO	19	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.1
ORG_PRO	19	Absence de politique de protection de l'information	ORG_15	BGC_MSS.3.1
ORG_PRO	19	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.4
ORG_PRO	19	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.2
ORG_PRO	19	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.4
ORG_PRO	19	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.2
ORG_PRO	19	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_PRO	19	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.3
ORG_PRO	20	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.2
ORG_PRO	20	Absence de politique de protection de l'information	ORG_15	BGC_MSS.3.1
ORG_PRO	20	Absence de politique de protection de l'information	ORG_15	BCM_CLI.2.1
ORG_PRO	20	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.2
ORG_PRO	20	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.1
ORG_PRO	20	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.4
ORG_PRO	20	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.4
ORG_PRO	20	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.3
ORG_PRO	20	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.1
ORG_PRO	20	Absence de politique de protection de l'information	ORG_15	BPS_PSI.1.5
ORG_PRO	20	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.2
ORG_PRO	21	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.2
ORG_PRO	21	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.4
ORG_PRO	21	Absence d'identification des besoins de sécurité d'un projet	ORG_32	BPS_PSI.2.2
ORG_PRO	21	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.4
ORG_PRO	21	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	21	Absence d'identification des besoins de sécurité d'un projet	ORG_32	CEI_ABS.1.1
ORG_PRO	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	FDP_RIP.1.1
ORG_PRO	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_PRO	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_PRO	22	Absence de contrôle des biens sensibles	ORG_04	BMA_IMT.2.1
ORG_PRO	22	Absence de contrôle des biens sensibles	ORG_04	BPE_MMG.2.1
ORG_PRO	22	Absence de contrôle des biens sensibles	ORG_04	BCM_RLC.1.1
ORG_PRO	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_PRO	22	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_PRO	22	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_PRO	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	BGC_MSS.2.1
ORG_PRO	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	BPE_SEM.6.1
ORG_PRO	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut	ORG_15	FDP_RIP.2.1
ORG_PRO	23	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.2.1
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.4.1
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.2
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_14	CGS_PAI.1.1
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	CGS_PAI.1.3
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	CGS_PAI.1.2
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.1.1
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	CGS_CIR.1.3
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BCM_CLI.1.2
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_SPR.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.1.1
ORG_PRO	23	Absence de politique de protection de l'information	ORG_15	BPS_PSI.1.5
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BPS_PSI.1.4
ORG_PRO	23	Absence de politique de protection de l'information	ORG_15	BGC_MSS.3.1
ORG_PRO	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.2.1
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_30	BMA_GAU.1.1
ORG_PRO	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.1.1
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information	ORG_14	BOS_ISI.3.1
ORG_PRO	23	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_PRO	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.4.1
ORG_PRO	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.1
ORG_PRO	23	Absence de politique de protection de l'information	ORG_15	BCM_CLI.1.2
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	BSP_SPR.3.1
ORG_PRO	23	Absence de contrôle des biens sensibles	ORG_15	BPE_MMG.1.1
ORG_PRO	23	Absence d'engagement personnel de protection de la confidentialité	ORG_37	BSP_SPR.3.1
ORG_PRO	23	Absence de contrôle des biens sensibles	ORG_15	BMA_IMT.2.1
ORG_PRO	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.4.1
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.1
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.1
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BCO_RPS.2.1
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BOS_ISI.3.1
ORG_PRO	23	Procédures de gestion et d'application des habilitations trop lourde à exploiter	ORG_36	CGS_GDH.1.3
ORG_PRO	23	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.3.1
ORG_PRO	23	Absence de contrôle des biens sensibles	ORG_15	BCM_CLI.2.1
ORG_PRO	23	Absence de contrôle des biens sensibles	ORG_15	BGC_MSS.1.1
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_15	CGS_CIR.1.2
ORG_PRO	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.1.1
ORG_PRO	23	Absence d'engagement personnel de protection de la confidentialité	PER_05	BSP_SPR.3.1
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous	ORG_14	BSP_SPR.4.1
ORG_PRO	23	La politique de sécurité n'est pas appliquée	ORG_18	BSP_RIS.5.2
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.3.1
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BGC_EIL.1.1
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BDM_SSA.3.1
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_GAU.2.1
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_MAS.2.1
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_MAS.3.1
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BSP_FOU.1.1
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BPS_PSI.1.3
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête	ORG_14	BMA_SAS.2.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.1
ORG_PRO	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_PRO	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_PRO	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.1.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.2.1
ORG_PRO	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	CET_EGT.1.3
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.2
ORG_PRO	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	CET_PLD.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	BOS_SAT.1.5
ORG_PRO	24	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.3
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.2
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.3
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.2
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.2.3
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.3.1
ORG_PRO	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet	ORG_33	BSP_SPR.3.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.4.1
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BGC_INT.2.1
ORG_PRO	25	Absence de procédures de qualification opérationnelle	ORG_26	BDM_SED.4.1
ORG_PRO	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_PRO	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_PRO	25	Logiciel non suffisamment recetté notamment dans le cadre des valeurs aux limites	ORG_26	BDM_SED.5.1
ORG_PRO	25	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_PRO	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	BOS_SAT.1.3
ORG_PRO	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	BDM_SED.4.1
ORG_PRO	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	BDM_ESS.1.1
ORG_PRO	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_PRO	25	Absence de contrôle des biens sensibles	ORG_04	BGC_MSS.3.1
ORG_PRO	25	Absence de contrôle des biens sensibles	ORG_04	BMA_IMT.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	25	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.3
ORG_PRO	25	Absence de contrôle des biens sensibles	ORG_04	BPE_MMG.1.1
ORG_PRO	25	Absence de contrôle des biens sensibles	ORG_04	BPE_MMG.2.1
ORG_PRO	25	Logiciel non suffisamment recetté notamment dans le cadre des valeurs aux limites	ORG_26	BGC_PRS.2.1
ORG_PRO	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance	ORG_20	CGS_OML.1.1
ORG_PRO	25	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.4
ORG_PRO	25	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_PRO	25	Absence de contrôle des biens sensibles	ORG_04	BGC_MSS.1.1
ORG_PRO	25	Absence de contrôle des biens sensibles	ORG_04	BCM_CLI.2.1
ORG_PRO	25	Absence de procédures de qualification opérationnelle	ORG_26	BDM_ESS.1.1
ORG_PRO	26	Absence de mesures de contrôle des développements	ORG_20	BDM_SFS.3.1
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation	ORG_04	CGS_PPS.2.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.2.1
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation	ORG_04	CGS_PPS.2.5
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.2
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.3
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.2
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.1.1
ORG_PRO	26	Absence de mesures de contrôle des développements	ORG_20	BDM_SED.5.1
ORG_PRO	26	Absence de mesures de contrôle des développements	ORG_20	BDM_SED.4.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BGC_INT.2.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	BMA_SAS.3.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.1
ORG_PRO	26	Absence d'identification des biens sensibles	ORG_26	BCM_RLC.1.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.1
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation	ORG_20	BDM_SED.5.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.3.3
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_SAA.2.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.3.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.2.3
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation	ORG_20	BDM_SED.2.1
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation	ORG_04	BDM_SFS.1.1
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation	ORG_04	BDM_SED.3.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.4.1
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation	ORG_04	BDM_SFS.2.1
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités	ORG_39	FAU_STG.1/2.2
ORG_PRO	27	Absence de règles de protection en confidentialité des informations, exploitables pour localiser un personnel (demandes de billets, registre d'entrée/sortie…)	ORG_15	CPD_DGL.1.1
ORG_PRO	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	CGI_GIS.3.2
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.1
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.3
ORG_PRO	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	BOS_ISI.1.2
ORG_PRO	28	Absence de consignes de réaction rapide pour la protection des matériels en cas de dégât des eaux ou d'incendie	ORG_24	CCS_SIN.2.3
ORG_PRO	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_PRO	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.2
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.1
ORG_PRO	28	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements	ORG_09	CEI_ABS.1.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.1
ORG_PRO	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.3
ORG_PRO	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.5
ORG_PRO	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.6
ORG_PRO	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	ORG_04	CCS_CSG.1.7
ORG_PRO	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	CGI_GIS.3.1
ORG_PRO	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)	PHY_08	CCS_CSG.1.2
ORG_PRO	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.2
ORG_PRO	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	BPE_SEM.4.1
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.3
ORG_PRO	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	CGI_GIS.3.3
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.2
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	BPE_SEM.4.1
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.1
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.2
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.1.1
ORG_PRO	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_PRO	28	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_PRO	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)	ORG_21	BSP_RIS.4.1
ORG_PRO	28	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements	ORG_09	BGC_PRS.1.1
ORG_PRO	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.3.3
ORG_PRO	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.3.1
ORG_PRO	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.3.2
ORG_PRO	28	Absence d'organisation du suivi des contrats de maintenance	ORG_27	CGS_GMA.1.2
ORG_PRO	29	Absence de procédures de qualification opérationnelle	ORG_26	BDM_SED.4.1
ORG_PRO	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_PRO	29	Absence de reporting sur les dysfonctionnements	ORG_21	CGI_GIS.3.2
ORG_PRO	29	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.3
ORG_PRO	29	Absence de procédures de qualification opérationnelle	ORG_26	CGS_PPS.2.4
ORG_PRO	29	Absence de reporting sur les dysfonctionnements	ORG_21	CGI_GIS.3.3
ORG_PRO	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_PRO	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_PRO	29	Absence de reporting sur les dysfonctionnements	ORG_21	CGI_GIS.3.1
ORG_PRO	29	Absence de procédures de qualification opérationnelle	ORG_26	BDM_ESS.1.1
ORG_PRO	29	Absence de reporting sur les dysfonctionnements	ORG_21	BSP_RIS.4.1
ORG_PRO	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)	PHY_10	CIS_ADL.2.1
ORG_PRO	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)	ORG_04	BPE_SEM.1.1
ORG_PRO	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)	ORG_04	CCS_CSG.1.4
ORG_PRO	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_PRO	29	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	29	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements	ORG_09	BGC_PRS.1.1
ORG_PRO	29	Absence de reporting sur les dysfonctionnements	ORG_21	BOS_ISI.1.2
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BGC_PRS.1.1
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	CGI_GIS.3.1
ORG_PRO	30	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements conduisant à la saturation des espaces de stockage ou des ressources de traitement	ORG_09	CCS_CSG.1.2
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	CGI_GIS.3.3
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BCA_AGC.3.1
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BCA_AGC.1.1
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	CGI_GIS.3.2
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours	ORG_09	BCA_AGC.5.1
ORG_PRO	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_PRO	31	Logiciel non suffisamment recetté (ensemble de jeux de test ne couvrant pas la totalité des conditions de fonctionnement -sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_26	BDM_SED.5.1
ORG_PRO	31	Logiciel non suffisamment recetté (ensemble de jeux de test ne couvrant pas la totalité des conditions de fonctionnement -sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_26	BGC_PRS.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_PRO	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.7
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.5
ORG_PRO	31	Logiciel non suffisamment recetté (ensemble de jeux de test ne couvrant pas la totalité des conditions de fonctionnement -sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_26	CGS_REC.1.1
ORG_PRO	31	Logiciel non suffisamment recetté (ensemble de jeux de test ne couvrant pas la totalité des conditions de fonctionnement -sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_26	BDM_SFS.1.1
ORG_PRO	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_PRO	31	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.3
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.2
ORG_PRO	31	Logiciel non suffisamment recetté (ensemble de jeux de test ne couvrant pas la totalité des conditions de fonctionnement -sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_26	BDM_ESS.1.1
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.6
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.1
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque	ORG_04	CCS_CSG.1.4
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.2
ORG_PRO	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	BGC_PRE.2.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	BCM_RLC.1.1
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	CGS_GMA.4.1
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BGC_MSS.4.1
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.1.1
ORG_PRO	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.1.1
ORG_PRO	32	Non-utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	BDM_SED.5.1
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BCM_RLC.1.1
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.1
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.2
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.1
ORG_PRO	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.4.1
ORG_PRO	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.3.1
ORG_PRO	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.2.1
ORG_PRO	32	Non-utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	BCO_RPS.2.1
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	BPE_SEM.4.1
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.4
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.1.2
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.5
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.2.1
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.1
ORG_PRO	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	BGC_PRE.2.1
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	32	Absence de procédures de gestion en configuration des systèmes	LOG_08	CDO_SDC.1.1
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.3
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.2
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.2.1
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BOS_SAT.1.1
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes	ORG_30	BMA_MAR.5.1
ORG_PRO	32	Absence de plan de reprise des activités essentielles de l'organisme	ORG_16	BCA_AGC.5.1
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GSU.3.2
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.7
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs	ORG_27	CGS_GMA.3.3
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.1
ORG_PRO	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.5
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.1.1
ORG_PRO	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.6
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.8
ORG_PRO	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.4
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BGC_PRE.3.1
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.6
ORG_PRO	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.1
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.5
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.4
ORG_PRO	32	Absence de plan de formation à la maintenance des nouveaux systèmes	ORG_14	CGS_GMA.2.1
ORG_PRO	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.2
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.3
ORG_PRO	32	Absence de Manuel d'Assurance Qualité	ORG_29	CPS_PAQ.1.3
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	CPS_DEV.1.2
ORG_PRO	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information	ORG_04	CPS_DEV.1.1
ORG_PRO	33	Absence de procédure de contrôle	ORG_33	BDM_SSA.4.1
ORG_PRO	33	Absence de sensibilisation sur les risques de sanction	ORG_37	BSP_RIS.5.1
ORG_PRO	33	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.1
ORG_PRO	33	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.2
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.7
ORG_PRO	33	Absence de procédure de contrôle	ORG_33	BDM_SSA.1.1
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.4
ORG_PRO	33	Absence de sensibilisation sur les risques de sanction	PER_08	BSP_RIS.5.2
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.5
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.2
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.3
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.6
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.1
ORG_PRO	34	Absence de sensibilisation sur les risques de sanction	PER_08	BSP_RIS.5.2
ORG_PRO	34	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.1
ORG_PRO	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.1.1
ORG_PRO	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BPS_PSI.1.3
ORG_PRO	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_41	BSP_FOU.1.1
ORG_PRO	34	Absence de procédure de contrôle	ORG_33	BCO_RPS.1.2
ORG_PRO	34	Absence de procédure de contrôle	ORG_33	BDM_SSA.1.1
ORG_PRO	34	Absence de procédure de contrôle	ORG_33	BDM_SSA.4.1
ORG_PRO	34	Absence de sensibilisation sur les risques de sanction	ORG_37	BSP_RIS.5.1
ORG_PRO	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.2.1
ORG_PRO	35	Absence de définition de privilèges limitant la possibilité d'installation sur les postes de travail	LOG_11	CGS_PPS.2.1
ORG_PRO	35	Absence de définition de privilèges limitant la possibilité d'installation sur les postes de travail	LOG_11	BDM_SFS.1.1
ORG_PRO	35	Absence de définition de privilèges limitant la possibilité d'installation sur les postes de travail	ORG_33	CGS_GLI.2.1
ORG_PRO	35	Absence de définition de privilèges limitant la possibilité d'installation sur les postes de travail	ORG_33	CGS_PPS.2.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	35	Absence de définition de privilèges limitant la possibilité d'installation sur les postes de travail	ORG_33	BMA_GAU.2.1
ORG_PRO	35	Absence de définition de privilèges limitant la possibilité d'installation sur les postes de travail	ORG_33	BMA_MAS.5.1
ORG_PRO	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_41	BSP_FOU.1.1
ORG_PRO	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.2.1
ORG_PRO	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BCO_CEL.1.1
ORG_PRO	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur	ORG_40	BPS_PSI.1.3
ORG_PRO	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.2.1
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.1
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.2
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.3
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.4
ORG_PRO	36	Absence de plan de formation sur les problèmes de sécurité	PER_02	BSP_FOU.1.1
ORG_PRO	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.1
ORG_PRO	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BOS_ISI.7.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BOS_SAT.1.3
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.6
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.7
ORG_PRO	36	Absence de contrôle de l'application de la politique de sécurité	ORG_22	BCO_RPS.1.2
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique	ORG_04	CCS_CSG.1.5
ORG_PRO	36	Absence de politique des habilitations d'accès à l'information	ORG_30	BMA_GAU.1.1
ORG_PRO	36	Absence de procédures de contrôle des disquettes extérieures	ORG_06	BGC_MSS.1.1
ORG_PRO	36	Absence de procédures de contrôle des disquettes extérieures	ORG_06	BGC_PLM.1.1
ORG_PRO	36	Absence de prévention et la détection des virus et d'autres logiciels malveillants	ORG_06	BGC_PLM.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.4
ORG_PRO	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.2
ORG_PRO	36	Absence de politique des habilitations d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_SEM.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.7.1
ORG_PRO	36	Absence de charte informatique précisant les exigences d'utilisation	ORG_04	CCS_CHI.1.1
ORG_PRO	36	Absence de plan de formation sur les problèmes de sécurité	PER_02	CFO_SPS.1.1
ORG_PRO	36	Absence de plan de formation sur les problèmes de sécurité	PER_02	CRR_SEN.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	CEI_ABS.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_SAS.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BOS_SAT.1.1
ORG_PRO	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BOS_SAT.1.3
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_SAS.2.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAS.2.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.4.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.3.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_EMA.1.1
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BGC_GER.1.1
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.2
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BGC_PRE.3.1
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.2.1
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	BSP_RIS.1.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	PER_08	BMA_MAS.6.1
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.8
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.7
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.6
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.5
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.3
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	PER_08	BSP_RIS.5.1
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.1
ORG_PRO	37	Absence de protection et d'audit d'accès aux informations sensibles	ORG_15	BCO_CEL.5.1
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)	ORG_24	CGI_GIS.1.4
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.1.1
ORG_PRO	37	Absence de protection et d'audit d'accès aux informations sensibles	ORG_35	BMA_SAS.2.1
ORG_PRO	37	Absence de protection et d'audit d'accès aux informations sensibles	ORG_35	BMA_SAS.1.1
ORG_PRO	37	Absence de protection et d'audit d'accès aux informations sensibles	ORG_15	CGS_GDH.1.1
ORG_PRO	37	Absence de protection et d'audit d'accès aux informations sensibles	ORG_15	BCM_CLI.1.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BOS_SAT.2.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BOS_SAT.1.3
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	PER_08	BSP_RIS.5.2
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.2.1
ORG_PRO	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_15	CGS_CIR.1.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_MAS.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.7.2
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.7.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.4.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.1.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BDM_SSA.1.1
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.3.1
ORG_PRO	37	Absence de sensibilisation du personnel	PER_05	BSP_SPR.4.1
ORG_PRO	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.5.1
ORG_PRO	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.4.1
ORG_PRO	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_40	BCO_CEL.1.1
ORG_PRO	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information	ORG_41	BPS_PSI.1.3
ORG_PRO	37	Absence de sensibilisation du personnel	ORG_14	BSP_FOU.1.1
ORG_PRO	37	Absence de sensibilisation du personnel	ORG_14	BSP_SPR.4.1
ORG_PRO	37	Absence de protection et d'audit d'accès aux informations sensibles	ORG_35	BMA_SAS.3.1
ORG_PRO	37	Absence de sensibilisation du personnel	ORG_14	BSP_SPR.1.1
ORG_PRO	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_15	BCO_CEL.4.1
ORG_PRO	37	Absence de sensibilisation du personnel	PER_05	BSP_SPR.3.1
ORG_PRO	37	Absence de sensibilisation du personnel	PER_05	BSP_SPR.1.1
ORG_PRO	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_14	BCM_CLI.1.2
ORG_PRO	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_14	CGS_PAI.1.1
ORG_PRO	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_14	CGS_CIR.1.3
ORG_PRO	37	Absence de responsable de la protection des données et des informations liées aux individus	ORG_15	CGS_CIR.1.2
ORG_PRO	37	Absence de dispositif de contrôle et de sanction	ORG_37	BDM_SSA.4.1
ORG_PRO	37	Absence de sensibilisation du personnel	ORG_14	BSP_SPR.3.1
ORG_PRO	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.2
ORG_PRO	38	Absence de formation sur les matériels ou logiciels utilisés	PER_12	BSP_FOU.2.1
ORG_PRO	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.3
ORG_PRO	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.1
ORG_PRO	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.4
ORG_PRO	39	Absence d'un règlement définissant les droits	ORG_33	CGS_PAI.2.1
ORG_PRO	39	Absence de contrôle sur les attributions des droits des utilisateurs	LOG_11	BMA_GAU.4.1
ORG_PRO	39	Absence de définition du droit d'en connaître	ORG_33	CGS_PAI.2.2
ORG_PRO	39	Absence d'un règlement définissant les droits	ORG_33	CGS_PAI.2.3
ORG_PRO	40	Absence de procédure d'habilitation du personnel	ORG_30	BMA_GAU.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAR.1.1
ORG_PRO	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.2
ORG_PRO	40	Absence de procédure d'habilitation du personnel	ORG_30	BMA_GAU.2.1
ORG_PRO	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAS.2.1
ORG_PRO	40	Organisation inadaptée	ORG_14	CGS_OES.1.1
ORG_PRO	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.1
ORG_PRO	40	Absence de climat de confiance entre les individus	ORG_37	BSP_RIS.5.2
ORG_PRO	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.4
ORG_PRO	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_MAS.1.1
ORG_PRO	40	Absence de climat de confiance entre les individus	ORG_37	BSP_RIS.5.1
ORG_PRO	40	Absence de climat de confiance entre les individus	PER_05	BSP_FOU.1.1
ORG_PRO	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_REU.2.1
ORG_PRO	40	Absence de procédure d'habilitation du personnel	LOG_11	CGS_PPS.2.1
ORG_PRO	41	Changement de politique ou de stratégie d'organisation	ORG_33	CGS_OES.1.3
ORG_PRO	41	Changement de politique ou de stratégie d'organisation	ORG_33	CGS_OES.1.2
ORG_PRO	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAR.1.1
ORG_PRO	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAS.2.1
ORG_PRO	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_MAS.1.1
ORG_PRO	41	Changement de politique ou de stratégie d'organisation	ORG_33	BMA_MAS.3.1
ORG_PRO	41	Absence d'organisation hiérarchique et de procédure de reporting	ORG_21	CGI_GIS.3.3
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BMA_SAS.3.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BMA_SAS.2.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BMA_SAS.1.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.1/2.2
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.4.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.3.1
ORG_PRO	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_REU.2.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.2.2
ORG_PRO	41	Absence de définition des responsabilités	ORG_14	BOS_ISI.3.1
ORG_PRO	41	Absence de définition des responsabilités	ORG_14	BPS_PSI.1.3
ORG_PRO	41	Absence de définition des responsabilités	ORG_14	BSP_SPR.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	41	Absence de définition des responsabilités	ORG_14	BSP_SPR.4.1
ORG_PRO	41	Absence de fonctions d'audit séparées des fonctions de suivi	PER_07	BOS_ISI.7.1
ORG_PRO	41	Absence d'organisation hiérarchique et de procédure de reporting	ORG_21	CGI_GIS.3.1
ORG_PRO	41	Absence d'organisation hiérarchique et de procédure de reporting	ORG_21	CGI_GIS.3.2
ORG_PRO	41	Absence de fonctions d'audit séparées des fonctions de suivi	ORG_22	BOS_ISI.7.1
ORG_PRO	41	Absence d'organisation hiérarchique et de procédure de reporting	ORG_21	BSP_RIS.4.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.2.1
ORG_PRO	41	Absence de procédures disciplinaires	ORG_37	BSP_RIS.5.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.2.3
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.3.1
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.3.2
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_SAA.3.3
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.1/2.1
ORG_PRO	41	Absence d'organisation hiérarchique et de procédure de reporting	ORG_21	BOS_ISI.1.2
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	FAU_STG.2.3
ORG_PRO	41	Absence de procédures disciplinaires	ORG_37	BSP_RIS.5.2
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes	ORG_39	BGC_INT.2.1
ORG_PRO	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.4
ORG_PRO	42	Absence de base documentaire des règles et procédures	ORG_41	BGC_PRE.1.1
ORG_PRO	42	Absence d'organisation redondante des fonctions sensibles	ORG_14	CFO_FRS.1.5
ORG_PRO	42	Absence de processus de gestion de la continuité des activités professionnelles de l'équipe projet	ORG_16	BCA_AGC.1.1
ORG_PRO	42	Absence de processus de gestion de la continuité des activités professionnelles de l'équipe projet	ORG_16	BCA_AGC.2.1
ORG_PRO	42	Absence de processus de gestion de la continuité des activités professionnelles de l'équipe projet	ORG_16	BCA_AGC.3.1
ORG_PRO	42	Absence de processus de gestion de la continuité des activités professionnelles de l'équipe projet	ORG_16	BCA_AGC.4.1
ORG_PRO	42	Absence de processus de gestion de la continuité des activités professionnelles de l'équipe projet	ORG_16	BCA_AGC.5.1
ORG_PRO	42	Absence d'organisation redondante des fonctions sensibles	PER_04	CFO_FRS.1.1
ORG_PRO	42	Absence d'organisation redondante des fonctions sensibles	PER_04	CFO_FRS.1.4

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_PRO	42	Absence d'organisation redondante des fonctions sensibles	ORG_14	CFO_FRS.1.2
ORG_PRO	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.2
ORG_PRO	42	Absence d'organisation redondante des fonctions sensibles	ORG_14	CFO_FRS.1.3
ORG_PRO	42	Sous-dimensionnement de l'organisation	PER_04	CRH_DDE.1.2
ORG_PRO	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.1.1
ORG_PRO	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.2.1
ORG_PRO	42	Non-redondance du personnel stratégique	PER_04	CFO_FRS.1.2
ORG_PRO	42	Non-redondance du personnel stratégique	PER_04	CFO_FRS.1.4
ORG_PRO	42	Non-redondance du personnel stratégique	PER_04	CFO_FRS.1.1
ORG_PRO	42	Sous-dimensionnement de l'organisation	ORG_14	CRH_DDE.1.2
ORG_PRO	42	Sous-dimensionnement de l'organisation	PER_04	CRH_DDE.1.1
ORG_PRO	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.3.1
ORG_PRO	42	Sous-dimensionnement de l'organisation	ORG_14	CRH_DDE.1.1
ORG_PRO	42	Non-redondance du personnel stratégique	PER_04	CFO_FRS.1.3
ORG_PRO	42	Non-redondance du personnel stratégique	PER_04	CFO_FRS.1.5
ORG_PRO	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.3
ORG_PRO	42	Absence de procédures de transfert de connaissances	PER_06	CFO_FRS.2.1
ORG_PRO	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	PER_10	BSP_FOU.1.1
ORG_PRO	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.5.1
ORG_PRO	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles	ORG_16	BCA_AGC.4.1

4.6.4 ORG_EXT : Sous-traitant/Fournisseurs/Industriels

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	1	Absence de consignes de sécurité fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CET_PLD.1.4
ORG_EXT	1	Absence de consignes de sécurité fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CET_EIP.1.1
ORG_EXT	1	Absence de clauses contractuelles pour le recouvrement des activités dans le cas d'une crise déclarée chez le fournisseur	ORG_38	BOS_SOT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	1	Absence de clauses contractuelles pour le recouvrement des activités dans le cas d'une crise déclarée chez le fournisseur	ORG_38	BGC_PRE.6.1
ORG_EXT	1	Absence de clauses contractuelles pour le recouvrement des activités dans le cas d'une crise déclarée chez le fournisseur	ORG_38	BOS_SOT.1.2
ORG_EXT	1	Absence de consignes de sécurité fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CCS_CSP.1.1
ORG_EXT	1	Absence de consignes de sécurité fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CCS_SIN.1.1
ORG_EXT	2	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	2	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	2	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	4	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	4	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	4	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	5	Absence de consignes fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CCS_SIN.1.1
ORG_EXT	5	Absence de consignes fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CET_EIP.1.1
ORG_EXT	5	Absence de consignes fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CET_PLD.1.4
ORG_EXT	5	Absence de consignes fournies aux personnes extérieures intervenant dans les locaux	ORG_25	CCS_CSP.1.1
ORG_EXT	6	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	6	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	6	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	7	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	7	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BGC_PRE.6.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	7	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	8	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	8	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	8	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	9	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	9	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	9	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	10	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	10	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	10	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	11	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BGC_PRE.6.1
ORG_EXT	11	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.2
ORG_EXT	11	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.1
ORG_EXT	11	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BGC_PRE.6.1
ORG_EXT	11	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.2
ORG_EXT	11	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.1
ORG_EXT	12	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	12	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.2
ORG_EXT	12	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.1
ORG_EXT	12	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BGC_PRE.6.1
ORG_EXT	12	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BGC_PRE.6.1
ORG_EXT	12	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.1
ORG_EXT	13	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.2
ORG_EXT	13	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.1
ORG_EXT	13	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BGC_PRE.6.1
ORG_EXT	13	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.1
ORG_EXT	13	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel	ORG_38	BGC_PRE.6.1
ORG_EXT	13	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel	ORG_38	BOS_SOT.1.2
ORG_EXT	14	Absence de clause contractuelle liée à la compatibilité électromagnétique	ORG_38	BOS_SOT.1.2
ORG_EXT	14	Absence de clause contractuelle liée à la compatibilité électromagnétique	ORG_38	BGC_PRE.6.1
ORG_EXT	14	Absence de clause contractuelle liée à la compatibilité électromagnétique	ORG_38	BOS_SOT.1.1
ORG_EXT	17	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	17	Absence de procédure de vérification des matériels avant achat ou après une maintenance	ORG_20	BDM_SED.4.1
ORG_EXT	17	Absence de procédure de vérification des matériels avant achat ou après une maintenance	ORG_20	BDM_SED.2.1
ORG_EXT	17	Absence de procédure de vérification des matériels avant achat ou après une maintenance	ORG_20	BGC_MSS.1.1
ORG_EXT	17	Absence de procédure de vérification des matériels avant achat ou après une maintenance	ORG_20	BDM_SED.1.1
ORG_EXT	17	Absence de procédure de vérification des matériels avant achat ou après une maintenance	ORG_20	BDM_ESS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	17	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	17	Absence de procédure de vérification des matériels avant achat ou après une maintenance	ORG_20	BDM_SFS.3.1
ORG_EXT	17	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	18	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	18	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	18	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	19	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	19	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	19	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	20	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	20	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	20	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	21	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BGC_PRE.6.1
ORG_EXT	21	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	21	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	22	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.1
ORG_EXT	22	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BGC_PRE.6.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	22	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs	ORG_38	BOS_SOT.1.2
ORG_EXT	24	Absence de moyens permettant de garantir la provenance des fournitures	ORG_20	BDM_SED.4.1
ORG_EXT	24	Absence de moyens permettant de garantir la provenance des fournitures	ORG_20	BDM_ESS.1.1
ORG_EXT	24	Absence de moyens permettant de garantir la provenance des fournitures	ORG_20	CGS_OML.1.1
ORG_EXT	25	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	BOS_SAT.1.3
ORG_EXT	25	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	CET_EIP.1.5
ORG_EXT	25	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	CET_EIP.1.3
ORG_EXT	25	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	CET_EIP.1.4
ORG_EXT	26	Absence de clauses contractuelles traitant de la garantie d'innocuité des fournitures livrées par le sous-traitant ou fournisseur	ORG_20	BGC_PLM.1.1
ORG_EXT	26	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	BOS_SAT.1.3
ORG_EXT	26	Absence de clauses contractuelles traitant de la garantie d'innocuité des fournitures livrées par le sous-traitant ou fournisseur	ORG_38	BDM_SED.5.1
ORG_EXT	26	Absence de clauses contractuelles traitant de la garantie d'innocuité des fournitures livrées par le sous-traitant ou fournisseur	ORG_38	BGC_PRE.6.1
ORG_EXT	26	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	CET_EIP.1.5
ORG_EXT	26	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	CET_EIP.1.4
ORG_EXT	26	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme	ORG_25	CET_EIP.1.3
ORG_EXT	26	Absence de clauses contractuelles traitant de la garantie d'innocuité des fournitures livrées par le sous-traitant ou fournisseur	ORG_20	BDM_SED.4.1
ORG_EXT	28	Absence de clause traitant des délais d'intervention et de remplacement en cas de panne matérielle	ORG_38	BGC_PRE.6.1
ORG_EXT	28	Absence de clause traitant des délais d'intervention et de remplacement en cas de panne matérielle	ORG_38	BOS_SOT.1.2
ORG_EXT	28	Absence de clause traitant des délais d'intervention et de remplacement en cas de panne matérielle	ORG_38	BOS_SOT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	29	Absence de clause traitant des délais d'intervention et de traitement en cas de dysfonctionnement	ORG_38	BOS_SOT.1.2
ORG_EXT	29	Absence de clause traitant des délais d'intervention et de traitement en cas de dysfonctionnement	ORG_38	BOS_SOT.1.1
ORG_EXT	29	Absence de clause traitant des délais d'intervention et de traitement en cas de dysfonctionnement	ORG_38	BGC_PRE.6.1
ORG_EXT	30	Absence de clause contractuelle traitant de la qualité de service des systèmes placés dans des conditions limites (sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_38	BOS_SOT.1.1
ORG_EXT	30	Absence de clause contractuelle traitant de la qualité de service des systèmes placés dans des conditions limites (sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_38	BGC_PRE.6.1
ORG_EXT	30	Absence de clause contractuelle traitant de la qualité de service des systèmes placés dans des conditions limites (sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)	ORG_38	BOS_SOT.1.2
ORG_EXT	31	Absence des clauses contractuelles traitant des conditions de support et d'intervention	ORG_38	BOS_SOT.1.2
ORG_EXT	31	Absence des clauses contractuelles traitant des conditions de support et d'intervention	ORG_38	BGC_PRE.6.1
ORG_EXT	31	Absence des clauses contractuelles traitant des conditions de support et d'intervention	ORG_38	BOS_SOT.1.1
ORG_EXT	32	Absence de clause contractuelle assurant le recouvrement de l'activité (en cas de cessation de l'activité, en cas de faillite du fournisseur…)	ORG_38	BOS_SOT.1.1
ORG_EXT	32	Absence de clause contractuelle assurant le recouvrement de l'activité (en cas de cessation de l'activité, en cas de faillite du fournisseur…)	ORG_38	BOS_SOT.1.2
ORG_EXT	32	Absence de garantie relative à la pérennité de l'organisme	ORG_27	CCC_RGF.1.2
ORG_EXT	32	Absence de garantie relative à la pérennité de l'organisme	ORG_27	CCC_RGF.1.1
ORG_EXT	32	Absence de clause contractuelle assurant le recouvrement de l'activité (en cas de cessation de l'activité, en cas de faillite du fournisseur…)	ORG_38	BGC_PRE.6.1
ORG_EXT	33	Absence de sensibilisation sur les risques de sanction	PER_08	BSP_RIS.5.2
ORG_EXT	33	Absence de sensibilisation sur les risques de sanction	ORG_37	BSP_RIS.5.1
ORG_EXT	33	Absence de clauses relatives à l'utilisation du matériel informatique dans le contrat	ORG_04	BOS_SAT.2.1
ORG_EXT	33	Absence de clauses relatives à l'utilisation du matériel informatique dans le contrat	ORG_04	BOS_SAT.1.5
ORG_EXT	33	Absence de clauses relatives à l'utilisation du matériel informatique dans le contrat	ORG_04	CCS_CHI.1.1
ORG_EXT	34	Absence de clauses sur l'utilisation de copie frauduleuse de logiciels dans le contrat	ORG_38	BGC_PRE.6.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	34	Absence de clauses sur l'utilisation de copie frauduleuse de logiciels dans le contrat	ORG_40	BCO_CEL.2.1
ORG_EXT	34	Absence de clauses sur l'utilisation de copie frauduleuse de logiciels dans le contrat	ORG_38	BDM_SED.5.1
ORG_EXT	34	Absence de clauses sur l'utilisation de copie frauduleuse de logiciels dans le contrat	ORG_38	BGC_PRE.6.1
ORG_EXT	35	Absence de clauses sur l'identification et la vérification de l'origine du logiciel dans le contrat	ORG_38	BOS_SOT.1.1
ORG_EXT	35	Absence de clauses sur l'identification et la vérification de l'origine du logiciel dans le contrat	ORG_38	BGC_PRE.6.1
ORG_EXT	35	Absence de clauses sur l'identification et la vérification de l'origine du logiciel dans le contrat	ORG_38	BOS_SOT.1.2
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_SAS.2.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.1.1
ORG_EXT	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BOS_SAT.1.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BOS_SAT.1.3
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.5.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_EMA.1.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BGC_GER.1.1
ORG_EXT	36	Absence de clauses relatives à la protection du matériel informatique dans le contrat	ORG_38	BOS_SOT.1.2
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.2.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.2.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.3.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	CEI_ABS.1.1
ORG_EXT	36	Absence de clauses relatives à la protection du matériel informatique dans le contrat	ORG_38	BOS_SOT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	36	Absence de clauses relatives à la protection du matériel informatique dans le contrat	ORG_38	BGC_PRE.6.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.1.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.4.1
ORG_EXT	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.2
ORG_EXT	36	Absence de politique des habilitations d'accès à l'information	ORG_30	CGS_GDH.1.4
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.2.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.3.1
ORG_EXT	36	Absence de politique des habilitations d'accès à l'information	ORG_30	BMA_GAU.2.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.3.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.5.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.4.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.3.1
ORG_EXT	36	Absence de politique des habilitations d'accès à l'information	ORG_30	BMA_GAU.1.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.2.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.4.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_SEM.1.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.4.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BPE_ZOS.5.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_SAS.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAS.2.1
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité…)	ORG_30	BMA_MAR.7.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.3.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	PER_08	BSP_RIS.5.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.4.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.1.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_SAS.2.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BOS_SAT.1.3
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	PER_08	BMA_MAS.6.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.7.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BMA_MAS.3.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BOS_SAT.2.1
ORG_EXT	37	Absence de clause de confidentialité dans le contrat	PER_09	BGC_PRE.6.1
ORG_EXT	37	Absence de clause de confidentialité dans le contrat	PER_09	BOS_SOT.1.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BDM_SSA.4.1
ORG_EXT	37	Absence de clause de confidentialité dans le contrat	PER_09	BOS_SOT.1.2
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.7.2
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	PER_08	BSP_RIS.5.2
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BDM_SSA.1.1
ORG_EXT	37	Absence de dispositif de contrôle et de sanction	ORG_37	BCO_CEL.1.1
ORG_EXT	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.4
ORG_EXT	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.3
ORG_EXT	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.2
ORG_EXT	38	Absence de double contrôle sur les processus critiques	ORG_43	CGS_GPC.2.1
ORG_EXT	39	Absence des clauses contractuelles limitant les responsabilités des 2 parties	ORG_38	CCC_CLR.1.2
ORG_EXT	39	Absence des clauses contractuelles limitant les responsabilités des 2 parties	ORG_38	BOS_SOT.1.2
ORG_EXT	39	Absence des clauses contractuelles limitant les responsabilités des 2 parties	ORG_38	BOS_SOT.1.1
ORG_EXT	39	Absence des clauses contractuelles limitant les responsabilités des 2 parties	ORG_38	BGC_PRE.6.1
ORG_EXT	40	Absence de procédure d'habilitation du personnel	ORG_30	BOS_SAT.1.5
ORG_EXT	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAR.1.1
ORG_EXT	40	Absence de procédure d'habilitation du personnel	ORG_30	BMA_GAU.1.1
ORG_EXT	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.4
ORG_EXT	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BOS_SAT.1.5
ORG_EXT	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BOS_SAT.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	LOG_11	BMA_MAS.2.1
ORG_EXT	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.1
ORG_EXT	40	Absence de protection des espaces dédiés à l'échange ou au partage d'information	ORG_30	CGS_PEP.1.1
ORG_EXT	40	Absence de procédure d'habilitation du personnel	ORG_30	BMA_GAU.2.1
ORG_EXT	40	Absence de procédure d'habilitation du personnel	LOG_11	CGS_PPS.2.1
ORG_EXT	40	Absence de procédure d'habilitation du personnel	ORG_30	CGS_GDH.1.2
ORG_EXT	40	Absence de procédure d'habilitation du personnel	ORG_30	BOS_SAT.1.2
ORG_EXT	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_MAS.1.1
ORG_EXT	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)	ORG_33	BMA_REU.2.1
ORG_EXT	41	Absence de clause relative à la définition des procédures de communication et d'échange dans le contrat	ORG_38	BGC_PRE.6.1
ORG_EXT	41	Présence de clause de pénalité ou de sanction démesurée ou non adaptée au contexte	ORG_38	BGC_PRE.6.1
ORG_EXT	41	Présence de clause de pénalité ou de sanction démesurée ou non adaptée au contexte	ORG_37	CCC_CLR.1.1
ORG_EXT	41	Absence de clause relative à la définition des procédures de communication et d'échange dans le contrat	ORG_38	BOS_SOT.1.2
ORG_EXT	41	Présence de clause de pénalité ou de sanction démesurée ou non adaptée au contexte	ORG_38	BOS_SOT.1.2
ORG_EXT	41	Absence de clause relative à la définition des procédures de communication et d'échange dans le contrat	ORG_03	BGC_EIL.1.1
ORG_EXT	41	Présence de clause de pénalité ou de sanction démesurée ou non adaptée au contexte	ORG_38	BOS_SOT.1.1
ORG_EXT	41	Absence de clause relative à la définition des procédures de communication et d'échange dans le contrat	ORG_38	BOS_SOT.1.1
ORG_EXT	41	Absence de contrôle mutuel des codes	ORG_38	BOS_SOT.1.2
ORG_EXT	41	Absence de contrôle mutuel des codes	ORG_38	BOS_SOT.1.1
ORG_EXT	41	Absence de clause relative à la définition des procédures de communication et d'échange dans le contrat	ORG_03	BGC_EIL.7.1
ORG_EXT	41	Absence de contrôle mutuel des codes	ORG_38	BGC_PRE.6.1
ORG_EXT	41	Absence de contrôle mutuel des codes	ORG_20	BDM_SED.5.1
ORG_EXT	41	Absence de clause relative à la définition des procédures de communication et d'échange dans le contrat	ORG_03	BGC_EIL.4.1
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_16	BCA_AGC.1.1
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances	ORG_38	BOS_SOT.1.2
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances	PER_06	CFO_FRS.2.1
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances	PER_06	CFO_FRS.2.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances	PER_06	CFO_FRS.2.3
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances	PER_06	CFO_FRS.2.4
ORG_EXT	42	Absence de pérennité financière ou technologique de l'organisme	ORG_13	CCC_RGF.1.1
ORG_EXT	42	Absence de pérennité financière ou technologique de l'organisme	ORG_13	CCC_RGF.1.2
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_16	BCA_AGC.4.1
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances	ORG_38	BGC_PRE.6.1
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_16	BCA_AGC.2.1
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_38	BOS_SOT.1.2
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_38	BOS_SOT.1.1
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_16	BCA_AGC.3.1
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_38	BGC_PRE.6.1
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances	ORG_38	BOS_SOT.1.1
ORG_EXT	42	Absence de clause de continuité de la fourniture du service	ORG_16	BCA_AGC.5.1

4.7 SYS : Système

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS	19	Circulation en clair des échanges	RES_02	BPE_SEM.3.1
SYS	19	Circulation en clair des échanges	RES_02	BDM_COC.1.1
SYS	19	Circulation en clair des échanges	RES_02	FDP_UCT.1.1
SYS	19	Circulation en clair des échanges	RES_02	BGC_GER.1.1
SYS	19	Circulation en clair des échanges	RES_02	BDM_COC.5.1
SYS	19	Circulation en clair des échanges	RES_02	FCS_COP.1.1
SYS	19	Circulation en clair des échanges	RES_02	FDP_ITT.1/2.1
SYS	19	Circulation en clair des échanges	RES_02	BDM_COC.2.1
SYS	23	Le système est connecté à des réseaux externes	RES_02	FTA_TAB.1.1
SYS	23	Le système est connecté à des réseaux externes	RES_02	BPE_SEM.1.1
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)	ORG_04	BGC_PRE.2.2
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)	ORG_04	CDO_SDC.1.1
SYS	32	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2
SYS	32	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)	ORG_04	BCM_RLC.1.1
SYS	32	Utilisation de système obsolète	LOG_09	CEI_CDT.1.1
SYS	32	Absence de moyen de support interne	ORG_27	CGS_GSU.1.1
SYS	32	Absence de moyen de support interne	ORG_27	CGS_GSU.1.2
SYS	32	Absence de moyen de support interne	ORG_27	CGS_GSU.2.1
SYS	32	Absence de moyen de support interne	ORG_27	CGS_GSU.2.2
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)	ORG_04	CET_EIP.1.5
SYS	32	Utilisation de système non standard	ORG_28	CGS_PPS.2.3
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)	ORG_04	CET_EIP.1.3
SYS	32	Utilisation de système obsolète	LOG_09	CEI_CDT.1.2
SYS	32	Utilisation d'une version obsolète du serveur de messagerie	LOG_09	CEI_CDT.1.1
SYS	32	Utilisation d'une version obsolète du serveur de messagerie	LOG_09	CEI_CDT.1.2
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)	ORG_04	CET_EIP.1.6
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)	ORG_04	CET_EIP.1.4
SYS	32	Absence de moyen de support interne	ORG_27	CGS_GSU.2.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_GEN.1.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.1.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	BMA_SAS.1.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	BMA_SAS.2.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	BMA_SAS.3.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_GEN.1.2
SYS	33	Le dispositif utilisé permet un autre usage que celui qui est prévu	PER_03	CGS_GDH.2.1
SYS	33	Le dispositif utilisé permet un autre usage que celui qui est prévu	PER_03	CGS_GDH.1.2
SYS	33	Le dispositif est connecté à des réseaux externes	RES_01	BPE_SEM.1.1
SYS	33	Le dispositif est connecté à des réseaux externes	RES_01	FTA_TAB.1.1
SYS	33	Le dispositif est accessible par tous	LOG_11	CGS_GDH.2.1
SYS	33	Le dispositif est accessible par tous	LOG_11	CGS_GDH.1.2
SYS	33	Le dispositif est accessible par tous	ORG_01	CGS_GDH.2.1
SYS	33	Le dispositif est accessible par tous	ORG_01	CGS_GDH.1.2
SYS	33	Absence de règle d'accès	LOG_11	BMA_GAU.2.1
SYS	33	Absence de règle d'accès	LOG_11	BMA_GAU.1.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.4.3
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_GEN.2.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.1.2
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	BDM_COC.4.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_ARP.1.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.4.2
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.3.3
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.3.2
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.3.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.2.3
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.2.2
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	FAU_SAA.2.1
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)	ORG_22	BOS_SAT.1.1
SYS	34	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs	ORG_20	BDM_SED.4.1
SYS	34	Le dispositif d'accès permet le stockage de logiciels	RES_01	CGS_CSR.1.3
SYS	34	Le dispositif d'accès permet le téléchargement de logiciels	RES_01	CGS_CSR.1.3
SYS	34	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs	ORG_20	BGC_PRS.2.1
SYS	34	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs	ORG_20	CGS_OML.1.1
SYS	35	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs	ORG_20	CGS_OML.1.1
SYS	35	Le dispositif d'accès permet le stockage de logiciels	RES_01	CGS_CSR.1.3
SYS	35	Le dispositif d'accès permet le téléchargement de logiciels	RES_01	CGS_CSR.1.3
SYS	35	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs	ORG_20	BGC_PRS.2.1
SYS	35	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs	ORG_20	BDM_SED.4.1
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BCM_CLI.2.1
SYS	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.1.1
SYS	38	Absence de responsabilité	ORG_14	BSP_SPR.4.1
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.1.2
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BGC_MSS.3.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BPS_PSI.1.5
SYS	38	Insuffisance de compétence pour l'utilisateur	PER_12	BSP_FOU.2.1
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.3
SYS	38	Absence de responsabilité	ORG_14	BSP_SPR.1.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BCO_CEL.5.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BPE_SEM.6.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.2
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.3.1
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.3
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	FDP_RIP.1.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	FDP_RIP.2.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BGC_MSS.2.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BCM_CLI.1.1
SYS	38	Absence d'outil de supervision	MAT_13	CGS_SUP.1.1
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.1
SYS	38	Absence de mesure de protection (lecture seule…)	LOG_11	BCM_CLI.1.2
SYS	38	Absence de support à l'utilisateur accessible	ORG_27	CGS_GSU.2.2
SYS	39	Le dispositif est accessible par tous	LOG_11	CGS_GDH.1.2
SYS	39	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
SYS	39	Le principe du moindre privilège n'est pas appliqué	LOG_11	CGS_GDH.1.2
SYS	39	Le dispositif est accessible par tous	LOG_11	CGS_GDH.2.1
SYS	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
SYS	39	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
SYS	39	Le principe du moindre privilège n'est pas appliqué	LOG_11	CGS_GDH.2.1
SYS	39	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
SYS	41	Le dispositif est connecté à des réseaux externes	RES_03	BPE_SEM.1.1
SYS	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
SYS	41	Le dispositif d'accès ne journalise pas les traces issues de son exploitation	ORG_39	CGS_GDA.1.4
SYS	41	L'accès au dispositif de traces n'est pas protégé	LOG_11	CGS_GDT.1.1
SYS	41	L'accès au dispositif de traces n'est pas protégé	LOG_11	BCO_CEL.4.1
SYS	41	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
SYS	41	Le dispositif est accessible par tous (ex: dispositif n'authentifiant pas les postes client ni les utilisateurs)	LOG_11	CGS_GDH.2.1
SYS	41	Le dispositif est connecté à des réseaux externes	RES_03	FTA_TAB.1.1
SYS	41	Le dispositif est accessible par tous (ex: dispositif n'authentifiant pas les postes client ni les utilisateurs)	LOG_11	CGS_GDH.1.2
SYS	41	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
SYS	41	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2

4.7.1 SYS_INT : Dispositif d'accès Internet

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_INT	19	Absence de protection des journaux récoltant la trace des activités	ORG_39	BDM_COC.2.1
SYS_INT	23	Absence de journalisation des accès	RES_03	CGS_GDA.1.3
SYS_INT	23	Absence de dispositif de filtrage	RES_02	CGS_CSR.1.2
SYS_INT	23	Absence de journalisation des accès	RES_03	BMA_MAS.3.1
SYS_INT	24	Le dispositif permet d'accéder à des données non authentifiables (ex. : hoax)	ORG_12	CCS_CSG.1.1
SYS_INT	24	Le dispositif permet d'accéder à des données non authentifiables (ex. : hoax)	ORG_12	CFO_SPS.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_INT	24	Le dispositif permet d'accéder à des données non authentifiables (ex. : hoax)	ORG_12	CFO_SPS.1.1
SYS_INT	24	Le dispositif permet d'accéder à des données non authentifiables (ex. : hoax)	ORG_12	CCS_CSG.1.2
SYS_INT	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.1/2.1
SYS_INT	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.1/2.2
SYS_INT	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.2.3
SYS_INT	26	Absence de contrôle anti-virus des échanges	ORG_06	BGC_PLM.1.1
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels	PER_03	BMA_MAS.5.1
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels	PER_03	BMA_GAU.2.1
SYS_INT	26	Le dispositif permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex. : composants javascript explorant le contenu du disque dur)	LOG_04	CGS_CSR.1.2
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels	PER_03	BDM_SED.4.1
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels	PER_03	CGS_PPS.2.3
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels	PER_03	CGS_OML.1.2
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels	PER_03	CGS_PPS.2.1
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels	PER_03	BDM_SFS.1.1
SYS_INT	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CGS_CSR.1.2
SYS_INT	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CEI_ABS.1.5
SYS_INT	30	Mauvais dimensionnement des ressources (ex. : trop d'utilisateurs par rapport aux nombres possibles de connexions et à la bande passante)	ORG_09	CEI_ABS.1.5
SYS_INT	30	Mauvais dimensionnement des ressources (ex. : trop d'utilisateurs par rapport aux nombres possibles de connexions et à la bande passante)	ORG_09	BGC_PRS.1.1
SYS_INT	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.4.1
SYS_INT	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BGC_PRE.2.2
SYS_INT	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.1
SYS_INT	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.1.1
SYS_INT	31	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CGS_CSR.1.2
SYS_INT	31	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CEI_ABS.1.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_INT	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.2
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BGC_PRE.2.1
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	CGS_PPS.2.1
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BGC_PRS.2.1
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.4.1
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.3.1
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.1.1
SYS_INT	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	CGS_PPS.2.3
SYS_INT	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	CGS_PPS.2.4
SYS_INT	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	BDM_SED.4.1
SYS_INT	36	Le dispositif permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex. : composants javascript explorant le contenu du disque dur)	LOG_11	CGS_CSR.1.2
SYS_INT	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	BGC_PLM.1.1
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.2.1
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.2.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.1
SYS_INT	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	CDP_INP.1.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.1
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.1.1
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.3
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.2
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.1
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.9
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.8
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.7
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.6
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.5
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.2.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.2
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.3
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	BDM_COC.4.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.3
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.2
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.3
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.2
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.2
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.3.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.2.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.1.1
SYS_INT	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_ARP.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.3
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CCS_SRI.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.3
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BCM_CLI.1.2
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BGC_EIL.6.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BOS_ISI.3.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.3.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.4.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CCS_SRI.1.1
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.2
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.2
SYS_INT	37	Le dispositif est connecté à des réseaux externes	RES_01	FTA_TAB.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BCM_CLI.1.2
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BGC_EIL.6.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BOS_ISI.3.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.4.1
SYS_INT	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	BGC_PRE.2.1
SYS_INT	37	Le dispositif est connecté à des réseaux externes	RES_01	BPE_SEM.1.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.2
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.4
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.4.1
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.1
SYS_INT	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.3
SYS_INT	37	Absence de contrôle de contenu	ORG_30	CGS_CSR.1.3
SYS_INT	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
SYS_INT	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.1.2
SYS_INT	40	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
SYS_INT	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	BDM_SSA.1.1
SYS_INT	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
SYS_INT	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
SYS_INT	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.2.1

4.7.2 SYS_MES : Messagerie

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	19	Possibilité d'introduire sur les clients un logiciel d'écoute	LOG_08	CGS_PPS.2.4
SYS_MES	19	Possibilité de pose d'un dispositif d'écoute logique sur les passerelles de messagerie	LOG_08	BDM_SED.4.1
SYS_MES	19	Possibilité de pose d'un dispositif d'écoute logique sur les passerelles de messagerie	LOG_08	CGS_PPS.2.4
SYS_MES	19	Possibilité de pose d'un dispositif d'écoute logique sur les passerelles de messagerie	LOG_08	CGS_PPS.2.3
SYS_MES	19	Possibilité d'introduire sur les clients un logiciel d'écoute	LOG_08	CGS_PPS.2.3
SYS_MES	19	Lacunes dans la gestion des privilèges d'accès aux passerelles de messagerie	LOG_11	CGS_PAI.1.2
SYS_MES	19	Possibilité d'introduire sur les clients un logiciel d'écoute	LOG_08	BDM_SED.4.1
SYS_MES	19	Lacunes dans la gestion des privilèges d'accès aux passerelles de messagerie	LOG_11	BMA_GAU.2.1
SYS_MES	19	Lacunes dans la gestion des privilèges d'accès aux passerelles de messagerie	LOG_11	BMA_GAU.4.1
SYS_MES	23	Le système est utilisable par tout le personnel	LOG_13	CGS_GDH.2.1
SYS_MES	23	Le système est utilisable par tout le personnel	LOG_13	CGS_GDH.1.2
SYS_MES	23	Absence de mesure permettant d'éviter une négligence lors de l'envoi d'informations	LOG_17	BGC_EIL.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	23	Absence de protection anti-virus efficace et opérationnelle	ORG_06	BGC_PLM.1.1
SYS_MES	23	Le système permet l'échange de pièces jointes	PER_02	BGC_EIL.4.1
SYS_MES	23	Le système permet l'échange de pièces jointes	PER_02	BGC_EIL.5.1
SYS_MES	23	Absence de mesure permettant d'éviter une négligence lors de l'envoi d'informations	LOG_17	BGC_EIL.5.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRR.1.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRR.1.2
SYS_MES	24	Le système ne dispose pas de filtre pour empêcher la réception de canulars provenant de l'extérieur	ORG_12	CGS_CSR.1.2
SYS_MES	24	Le système permet le relayage	RES_01	CGS_CSR.1.1
SYS_MES	24	Le système permet le relayage	RES_01	BGC_EIL.1.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRR.1.3
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	BMA_MAS.3.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRR.2.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRO.2.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	BMA_MAS.2.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRO.1.1
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRO.1.2
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires	RES_03	FCO_NRO.1.3
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.1.1
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BGC_PRS.2.1
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.1.1
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.2
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BGC_PRE.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BDM_SED.3.1
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BDM_SED.1.1
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	CGS_PPS.2.1
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.1
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BDM_SED.4.1
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BDM_SED.4.1
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BDM_SED.2.1
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.2.1
SYS_MES	26	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
SYS_MES	26	La liaison de télémaintenance est activée en permanence	RES_06	BDM_COC.4.1
SYS_MES	26	La liaison de télémaintenance est activée en permanence	RES_06	BMA_MAR.5.1
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)	LOG_11	BDM_SED.1.1
SYS_MES	26	La messagerie permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex: lancement automatique des pièces jointes)	LOG_04	CGS_CSR.1.2
SYS_MES	26	Utilisation d'une version obsolète du serveur de messagerie	LOG_09	CEI_CDT.1.1
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.2
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
SYS_MES	26	Présence de protocole ne disposant pas de fonction d'authentification	RES_03	BDM_COC.4.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	BGC_PLM.1.1
SYS_MES	26	La messagerie permet l'émission automatique de messages	ORG_06	BGC_EIL.4.1
SYS_MES	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1
SYS_MES	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.4.1
SYS_MES	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
SYS_MES	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BMA_MAR.4.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FTA_TSE.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MOF.1.1
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.1.1
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.3.2
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.1.1
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.2.1
SYS_MES	26	Utilisation de liste de diffusion incluant une grande partie des personnels	ORG_12	BGC_EIL.4.1
SYS_MES	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.1.1
SYS_MES	26	Absence de sensibilisation aux risques induits par l'exécution de pièces jointes	PER_03	CFO_SPS.1.1
SYS_MES	26	La messagerie permet l'émission automatique de messages	ORG_06	CGS_CME.1.1
SYS_MES	26	Utilisation de liste de diffusion incluant une grande partie des personnels	ORG_12	CGS_CME.1.1
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	CAR_PAR.1.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FMT_MOF.1.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	BDM_COC.4.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.3.2
SYS_MES	26	Utilisation d'une version obsolète du serveur de messagerie	LOG_09	CEI_CDT.1.2
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.2.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITA.1.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.2
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.2.3
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.1
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.2
SYS_MES	26	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.1.1
SYS_MES	26	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	CGS_OML.1.1
SYS_MES	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
SYS_MES	26	Absence de moyens de filtrage anti-virus	ORG_06	BGC_PLM.1.1
SYS_MES	26	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BDM_SED.4.1
SYS_MES	26	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PRS.2.1
SYS_MES	30	Absence de limitation des tailles des pièces jointes	LOG_14	BGC_EIL.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	30	Mauvais dimensionnement des espaces de stockage des messages reçus	ORG_09	BGC_PRS.1.1
SYS_MES	30	Mauvais dimensionnement des espaces de stockage des messages reçus	ORG_09	CEI_ABS.1.5
SYS_MES	30	Absence de protection contre le spam	ORG_12	CGS_CSR.1.2
SYS_MES	30	Mauvais usage des utilisateurs du service de messagerie (utilisation des boîtes aux lettres comme espace d'archivage)	PER_03	CCS_CSG.1.1
SYS_MES	30	Absence de limitation des tailles des pièces jointes	LOG_14	CGS_CME.1.1
SYS_MES	30	Utilisation de liste de diffusion interne accessibles à tous	ORG_12	CGS_CME.1.1
SYS_MES	30	Mauvais usage des utilisateurs du service de messagerie (utilisation des boîtes aux lettres comme espace d'archivage)	PER_03	CCS_CSG.1.2
SYS_MES	30	La messagerie permet l'émission automatique de messages	LOG_14	BGC_EIL.4.1
SYS_MES	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système	ORG_09	CDS_DES.1.1
SYS_MES	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système	ORG_09	CEI_ABS.1.5
SYS_MES	30	La messagerie permet l'émission automatique de messages	LOG_14	CGS_CME.1.1
SYS_MES	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BGC_PRE.2.2
SYS_MES	31	Incompatibilité logiciel (ex. : effet de bord d'un logiciel anti-virus filtrant les messages...)	RES_04	BGC_PRS.2.1
SYS_MES	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur SMTP, POP3, IMAP)	LOG_14	BDM_SSA.1.1
SYS_MES	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.1.1
SYS_MES	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.1
SYS_MES	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.4.1
SYS_MES	31	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PRS.2.1
SYS_MES	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.1
SYS_MES	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	LOG_09	CEI_CDT.1.2
SYS_MES	31	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BDM_SED.4.1
SYS_MES	31	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	CGS_OML.1.1
SYS_MES	31	Utilisation d'une version obsolète du serveur de messagerie	LOG_09	CEI_CDT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	31	Utilisation d'une version obsolète du serveur de messagerie	LOG_09	CEI_CDT.1.2
SYS_MES	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.2
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.3
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.1.1
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.2.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	BDM_COC.4.1
SYS_MES	36	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PRS.2.1
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	BGC_INT.1.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FTA_TSE.1.1
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.4
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.5
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.6
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FMT_MOF.1.1
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.8
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MOF.1.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	BGC_PLM.1.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.2.3
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.1.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.3.2
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.1.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.2.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FPT_ITA.1.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.1
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.3.2
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.2
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.1.1
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.1
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.2
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.1
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.2
SYS_MES	36	Possibilité d'administrer le système à distance	RES_01	CAR_PAR.1.1
SYS_MES	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.4.1
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	BGC_PRE.1.1
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.7

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.2
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.1
SYS_MES	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels	LOG_04	FMT_MSA.3.1
SYS_MES	36	La liaison de télémaintenance est activée en permanence	RES_06	BMA_MAR.5.1
SYS_MES	36	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	CGS_OML.1.1
SYS_MES	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1
SYS_MES	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.9
SYS_MES	36	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
SYS_MES	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
SYS_MES	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
SYS_MES	36	La couche SNMP est activée	RES_06	BDM_COC.4.1
SYS_MES	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BMA_MAR.4.1
SYS_MES	36	La couche SNMP est activée	LOG_12	FAU_SAA.2.3
SYS_MES	36	La liaison de télémaintenance est activée en permanence	RES_06	BDM_COC.4.1
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.1.1
SYS_MES	36	La messagerie permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex: lancement automatique des pièces jointes)	LOG_04	CGS_CSR.1.2
SYS_MES	36	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BDM_SED.4.1
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.2.1
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.1.1
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.7
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.6
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.5
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.8
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.2.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.1.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	BDM_COC.4.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.1
SYS_MES	37	Absence de contrôle de contenu	ORG_30	CGS_CSR.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.4.1
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.4
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.2
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.2
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.3
SYS_MES	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	CDP_INP.1.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.2
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.3
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.2
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.3
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.9
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.3
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.2
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.3
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.2
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.2
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.2.1
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.2
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.4.1
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.3.1
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.1
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.1.1
SYS_MES	37	Le dispositif est connecté à des réseaux externes	RES_01	BPE_SEM.1.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_ARP.1.1
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BOS_ISI.3.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.3.1
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BGC_EIL.6.1
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BCM_CLI.1.2
SYS_MES	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	BGC_PRE.2.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.2.1
SYS_MES	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.1
SYS_MES	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.1.1
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.3
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CCS_SRI.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	37	Le dispositif est connecté à des réseaux externes	RES_01	FTA_TAB.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	BGC_PLM.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.2.1
SYS_MES	40	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
SYS_MES	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	CAR_PAR.1.1
SYS_MES	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FMT_MOF.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FTA_TSE.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FMT_MTD.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	BDM_COC.4.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FPT_ITA.1.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.1/2.2
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FPT_ITI.2.3
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FPT_ITT.3.2
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	BMA_MAR.4.1
SYS_MES	40	Possibilité d'administrer le système à distance	RES_01	FMT_MSA.3.2
SYS_MES	40	Utilisation d'une version obsolète du serveur de messagerie	ORG_13	CEI_CDT.1.2
SYS_MES	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.4.1
SYS_MES	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.1.2
SYS_MES	40	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BGC_PRS.2.1
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.2.1
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MOF.1.1
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.1.1
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MSA.3.2
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.1.1
SYS_MES	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.2.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_MAS.4.1
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	FMT_MTD.2.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.1.1
SYS_MES	40	Utilisation d'une version obsolète du serveur de messagerie	ORG_13	CEI_CDT.1.1
SYS_MES	40	Le dispositif de messagerie est accessible depuis Internet	RES_01	CGS_GDA.1.1
SYS_MES	40	Le dispositif de messagerie est accessible depuis Internet	RES_01	BGC_EIL.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_MES	40	Le dispositif de messagerie est accessible depuis Internet	RES_01	CGS_CSR.1.2
SYS_MES	40	La liaison de télémaintenance est activée en permanence	RES_06	BMA_MAR.5.1
SYS_MES	40	La liaison de télémaintenance est activée en permanence	RES_06	BDM_COC.4.1
SYS_MES	40	La liaison de télémaintenance est activée en permanence	LOG_12	FAU_SAA.2.3
SYS_MES	40	La couche SNMP est activée	RES_06	BDM_COC.4.1
SYS_MES	40	La couche SNMP est activée	LOG_12	FAU_SAA.2.3
SYS_MES	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	BDM_SSA.1.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.1.1
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste	LOG_11	CGS_GDH.1.2
SYS_MES	40	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	CGS_OML.1.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	FIA_SOS.2.2
SYS_MES	40	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	ORG_13	CEI_CDT.1.2
SYS_MES	40	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs	ORG_13	CEI_CDT.1.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.2
SYS_MES	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BDM_COC.2.1
SYS_MES	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	BMA_MAR.4.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	CGS_GMP.1.1
SYS_MES	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITT.1/2.1
SYS_MES	40	Aucune vérification des applicatifs n'est faite avant l'installation	LOG_06	BDM_SED.4.1
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion	ORG_10	BMA_REU.2.1
SYS_MES	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés	RES_02	FPT_ITC.1.1
SYS_MES	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2

4.7.3 SYS_ITR : Intranet

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ITR	19	Absence de cloisonnement des réseaux de communication	RES_02	BGC_PRE.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'application	RES_02	BGC_GER.1.1
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'application	RES_02	FDP_ITT.1/2.1
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'authentification	RES_02	BGC_GER.1.1
SYS_ITR	19	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.1.1
SYS_ITR	19	Absence de protection des journaux récoltant la trace des activités	ORG_39	BDM_COC.2.1
SYS_ITR	19	Absence de cloisonnement des réseaux de communication	RES_02	BMA_EMA.1.1
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'application	RES_02	FDP_UCT.1.1
SYS_ITR	19	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.2.1
SYS_ITR	19	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.6.1
SYS_ITR	19	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.7.1
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'authentification	RES_02	FDP_UCT.1.1
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'authentification	RES_02	FDP_ITT.1/2.1
SYS_ITR	19	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.1.1
SYS_ITR	23	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.7.1
SYS_ITR	23	Absence de cloisonnement des réseaux de communication	RES_02	BMA_EMA.1.1
SYS_ITR	23	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.6.1
SYS_ITR	23	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.1.1
SYS_ITR	23	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.2.1
SYS_ITR	23	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.1.1
SYS_ITR	23	Absence ou difficulté à gérer les privilèges d'accès aux informations partagés (définition, mise en œuvre, contrôle)	LOG_11	CGS_PEP.1.1
SYS_ITR	23	Absence de cloisonnement des réseaux de communication	RES_02	BGC_PRE.4.1
SYS_ITR	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.1/2.2
SYS_ITR	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.1/2.1
SYS_ITR	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.2.3
SYS_ITR	24	Le système permet le stockage ou la modification d'information sans authentification de leurs auteurs	RES_03	BMA_MAS.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance	LOG_11	BDM_SED.1.1
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance	LOG_11	BDM_SED.3.1
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance	LOG_11	BGC_PRS.2.1
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance	LOG_11	BDM_SED.2.1
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance	LOG_11	BDM_SED.4.1
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance	LOG_11	CGS_PPS.2.1
SYS_ITR	26	Utilisation d'espace de stockage partagé	LOG_11	CGS_PEP.1.1
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance	LOG_11	BGC_PRE.2.1
SYS_ITR	30	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.6.1
SYS_ITR	30	Absence de cloisonnement des réseaux de communication	RES_02	BMA_EMA.1.1
SYS_ITR	30	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.1.1
SYS_ITR	30	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.2.1
SYS_ITR	30	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.1.1
SYS_ITR	30	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.7.1
SYS_ITR	30	Mauvais dimensionnement des ressources (ex: espace de stockage ou de partage de fichier trop limitée)	ORG_09	BGC_PRS.1.1
SYS_ITR	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CEI_ABS.1.5
SYS_ITR	30	Mauvais dimensionnement des ressources (ex: espace de stockage ou de partage de fichier trop limitée)	ORG_09	CEI_ABS.1.5
SYS_ITR	30	Absence de gestion des droits d'écriture sur les espaces de stockage partagés	LOG_11	CGS_PEP.1.1
SYS_ITR	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CGS_CSR.1.2
SYS_ITR	30	Absence de cloisonnement des réseaux de communication	RES_02	BGC_PRE.4.1
SYS_ITR	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.4.1
SYS_ITR	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.1.1
SYS_ITR	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.2
SYS_ITR	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.1
SYS_ITR	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BGC_PRE.2.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ITR	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur LDAP)	LOG_14	BDM_SSA.1.1
SYS_ITR	36	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.7.1
SYS_ITR	36	Absence de cloisonnement des réseaux de communication	RES_02	BMA_EMA.1.1
SYS_ITR	36	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.6.1
SYS_ITR	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	BGC_PLM.1.1
SYS_ITR	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	BDM_SED.4.1
SYS_ITR	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	CGS_PPS.2.4
SYS_ITR	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…	ORG_06	CGS_PPS.2.3
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.3
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.4
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.5
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.6
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.7
SYS_ITR	36	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.1.1
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.8
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.9
SYS_ITR	36	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAA.2.1
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.3.1
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	BGC_PRE.1.1
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	CGS_PPS.2.1
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.1.1
SYS_ITR	36	Absence de cloisonnement des réseaux de communication	RES_02	BMA_MAR.1.1
SYS_ITR	36	Absence de procédure de sauvegarde	ORG_08	BGC_INT.1.1
SYS_ITR	36	Le dispositif permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex. : composants javascript explorant le contenu du disque dur)	LOG_11	CGS_CSR.1.2
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.4.1
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BGC_PRE.2.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BGC_PRS.2.1
SYS_ITR	36	Absence de cloisonnement des réseaux de communication	RES_02	BGC_PRE.4.1
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance	LOG_11	BDM_SED.2.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_ARP.1.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.2
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.3
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.2.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.2
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.3
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.2
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.3
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.2
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.9
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.2
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.3.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.2.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.1.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	BDM_COC.4.1
SYS_ITR	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.4.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.2
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.3
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.5
SYS_ITR	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	CDP_INP.1.1
SYS_ITR	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	BGC_PRE.2.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.6
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.7
SYS_ITR	37	Le dispositif est connecté à des réseaux externes	RES_01	BPE_SEM.1.1
SYS_ITR	37	Le dispositif est connecté à des réseaux externes	RES_01	FTA_TAB.1.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.4
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.2.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.1.1
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.3
SYS_ITR	37	Absence de contrôle de contenu	ORG_30	CGS_CSR.1.3
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.8
SYS_ITR	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.2
SYS_ITR	40	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
SYS_ITR	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ITR	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
SYS_ITR	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
SYS_ITR	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
SYS_ITR	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.2.1
SYS_ITR	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	BDM_SSA.1.1

4.7.4 SYS_ANU : Annuaire d'entreprise

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ANU	23	Absence de contrôle d'accès aux informations stockés dans l'annuaire	LOG_11	BMA_MAS.3.1
SYS_ANU	23	Absence de contrôle d'accès aux informations stockés dans l'annuaire	LOG_11	BMA_MAS.2.1
SYS_ANU	23	Absence de contrôle d'accès aux informations stockés dans l'annuaire	LOG_11	BMA_MAR.7.1
SYS_ANU	23	Absence de contrôle d'accès aux informations stockés dans l'annuaire	LOG_11	BMA_GAU.2.1
SYS_ANU	23	Absence de contrôle d'accès aux informations stockés dans l'annuaire	LOG_11	CGS_GDH.1.1
SYS_ANU	23	Absence de contrôle d'accès aux informations stockés dans l'annuaire	LOG_11	BMA_MAA.1.1
SYS_ANU	24	Le système ne permet pas d'identifier l'auteur d'une modification	LOG_10	BMA_MAS.3.1
SYS_ANU	24	Possibilité d'usurper la fonction de l'annuaire	RES_01	CGS_GDA.3.2
SYS_ANU	24	Possibilité d'usurper la fonction de l'annuaire	RES_01	CGS_GDA.3.1
SYS_ANU	24	Possibilité d'usurper la fonction de l'annuaire	RES_01	CGS_GDA.1.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.1.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.1.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BGC_PRS.2.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.4.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BGC_PRS.2.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.4.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.2.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.1.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	CGS_PPS.2.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.1.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BGC_PRE.2.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	CGS_PPS.2.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.3.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.2.1
SYS_ANU	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_20	BDM_SED.4.1
SYS_ANU	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_20	BDM_SED.5.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.4.1
SYS_ANU	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_20	BDM_SFS.3.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.4.1
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BGC_PRE.2.1
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.3.1
SYS_ANU	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CEI_ABS.1.5
SYS_ANU	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CGS_CSR.1.2
SYS_ANU	30	Mauvais dimensionnement des ressources (ex: trop d'utilisateurs par rapport à la capacité maximale de l'annuaire)	ORG_09	BGC_PRS.1.1
SYS_ANU	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système	ORG_09	CDS_DES.1.1
SYS_ANU	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système	ORG_09	CEI_ABS.1.5
SYS_ANU	30	Mauvais dimensionnement des ressources (ex: trop d'utilisateurs par rapport à la capacité maximale de l'annuaire)	ORG_09	CEI_ABS.1.5
SYS_ANU	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BGC_PRE.2.2
SYS_ANU	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.4.1
SYS_ANU	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.1.1
SYS_ANU	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.1
SYS_ANU	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur LDAP)	LOG_14	BDM_SSA.1.1
SYS_ANU	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.2
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.6
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.7
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.5
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.9
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.8
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.4
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	BGC_INT.1.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	BGC_PRE.1.1
SYS_ANU	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.3
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.4
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.3
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.8
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.9
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.1
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.2
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_PAI.1.3
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.1.1
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.2.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.3.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.2
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.2
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.3
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.2.1
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	BMA_GAU.4.1
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.1
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.2
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.3
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.5
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.6
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.1
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.4.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.2
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_ARP.1.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.3
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.2
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.2.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.2
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.2
SYS_ANU	37	Le dispositif est connecté à des réseaux externes	RES_01	FTA_TAB.1.1
SYS_ANU	37	Le dispositif est connecté à des réseaux externes	RES_01	BPE_SEM.1.1
SYS_ANU	37	Absence de contrôle de contenu	ORG_30	CGS_CSR.1.3
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.3.1
SYS_ANU	37	Absence de gestion d'habilitation des accès	LOG_11	CGS_GDH.1.7
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BOS_ISI.3.1
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BGC_EIL.6.1
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.3

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.1
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	CCS_SRI.1.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.1.1
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.1.1
SYS_ANU	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	BGC_PRE.2.1
SYS_ANU	37	Absence d'identification des niveaux de protection des systèmes	ORG_22	CDP_INP.1.1
SYS_ANU	37	Absence d'audit ou de supervision des accès	ORG_22	BDM_COC.4.1
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations	PER_02	BCM_CLI.1.2
SYS_ANU	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
SYS_ANU	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
SYS_ANU	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.2.1
SYS_ANU	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.1.2
SYS_ANU	40	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
SYS_ANU	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)	LOG_14	BDM_SSA.1.1
SYS_ANU	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2

4.7.5 SYS_WEB : Portail externe

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_WEB	19	Absence de protection des journaux récoltant la trace des activités	ORG_39	BDM_COC.2.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.4.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BGC_EIL.6.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.3.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.2
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)	LOG_11	BMA_GAU.2.1
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)	LOG_11	CGS_PAI.1.1
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)	LOG_11	CGS_PAI.1.2

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)	LOG_11	CGS_PAI.1.3
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	CCS_SRI.1.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BCM_CLI.1.2
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)	LOG_11	BMA_GAU.4.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.1.1
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)	LOG_11	BMA_GAU.1.1
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)	LOG_11	BGC_EIL.6.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.4.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	CGS_CIR.1.3
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BOS_ISI.3.1
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations	PER_02	BSP_SPR.1.1
SYS_WEB	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.2.3
SYS_WEB	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.1/2.1
SYS_WEB	24	Le système ne permet pas l'identification de la personne ayant émis une requête	RES_03	BMA_MAS.3.1
SYS_WEB	24	Le système ne dispose pas de moyen de conservation de l'historique des activités	RES_03	FAU_STG.1/2.2
SYS_WEB	26	Possibilité de créer ou modifier des commandes systèmes	LOG_11	BDM_SFS.1.1
SYS_WEB	26	Possibilité de créer ou modifier des commandes systèmes	LOG_11	BMA_GAU.2.1
SYS_WEB	26	Possibilité de créer ou modifier des commandes systèmes	LOG_11	CGS_PPS.2.5
SYS_WEB	26	Possibilité de créer ou modifier des commandes systèmes	LOG_11	CGS_GLI.2.1
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BGC_PRE.2.1
SYS_WEB	26	Possibilité d'implanter des programmes pirates	LOG_11	CGS_PPS.2.1
SYS_WEB	26	Possibilité de créer ou modifier des commandes systèmes	LOG_11	CGS_PPS.2.1
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BGC_PRS.2.1
SYS_WEB	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_20	BDM_SFS.3.1
SYS_WEB	26	Possibilité d'implanter des programmes pirates	LOG_11	BDM_SED.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_WEB	26	Possibilité d'implanter des programmes pirates	LOG_11	BGC_PRS.2.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.1.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.2.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.4.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BGC_PRE.2.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	CGS_PPS.2.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.1.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.3.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BDM_SED.4.1
SYS_WEB	26	Possibilité d'implanter des programmes pirates	LOG_11	BGC_PRE.2.1
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.3.1
SYS_WEB	26	Possibilité d'implanter des programmes pirates	LOG_11	BDM_SED.3.1
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.2.1
SYS_WEB	26	Possibilité d'implanter des programmes pirates	LOG_11	BDM_SED.1.1
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.4.1
SYS_WEB	26	Possibilité de créer ou modifier des commandes systèmes	LOG_11	BMA_MAS.5.1
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs	LOG_11	CGS_PPS.2.1
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs	LOG_11	BDM_SED.1.1
SYS_WEB	26	Possibilité d'implanter des programmes pirates	LOG_11	BDM_SED.2.1
SYS_WEB	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_20	BDM_SED.5.1
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes	LOG_11	BGC_PRS.2.1
SYS_WEB	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement	ORG_20	BDM_SED.4.1
SYS_WEB	30	Accès public au portail	ORG_09	CDS_DES.1.1
SYS_WEB	30	Accès public au portail	ORG_09	CGS_CSR.1.2
SYS_WEB	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CEI_ABS.1.5
SYS_WEB	30	Mauvais dimensionnement des ressources (ex: trop de connexions simultanées)	ORG_09	CEI_ABS.1.5
SYS_WEB	30	Mauvais dimensionnement des ressources (ex: trop de connexions simultanées)	ORG_09	BGC_PRS.1.1
SYS_WEB	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système	ORG_09	CDS_DES.1.1
SYS_WEB	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système	ORG_09	CEI_ABS.1.5

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_WEB	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation	ORG_09	CGS_CSR.1.2
SYS_WEB	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur SMTP, POP3, IMAP)	LOG_14	BDM_SSA.1.1
SYS_WEB	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.4.1
SYS_WEB	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_SPR.1.1
SYS_WEB	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.2
SYS_WEB	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BGC_PRE.2.2
SYS_WEB	31	Non-respect des procédures d'installation ou de maintenance	ORG_04	BSP_RIS.5.1
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	BGC_PRE.1.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_ARP.1.1
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	BGC_INT.1.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.2
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.2.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.3
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.2
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.3
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.2
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.3
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.2
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.2
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.6
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	BDM_COC.4.1
SYS_WEB	36	Absence de règle d'accès	LOG_11	BMA_GAU.2.1
SYS_WEB	36	Absence de règle d'accès	LOG_11	BMA_GAU.1.1
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.9
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.1
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.7
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.3.1
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.5
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.4
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.3
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.1.1
SYS_WEB	36	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.2.1
SYS_WEB	36	Absence de procédure de sauvegarde	ORG_08	CGS_SVG.1.8
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.2.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.3
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	BDM_COC.4.1

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.1.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.2
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.2.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.2
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_GEN.1.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.3
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	BMA_SAS.3.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.4.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.3
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.2
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.3.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.2.2
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.2
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_SAA.1.1
SYS_WEB	37	Absence d'audit ou de supervision des accès	ORG_22	FAU_ARP.1.1
SYS_WEB	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.2.1
SYS_WEB	40	Absence de journalisation des événements	LOG_15	BMA_SAS.1.1
SYS_WEB	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.1
SYS_WEB	40	Absence de journalisation des événements	LOG_15	FAU_GEN.1.2
SYS_WEB	40	Absence de politique d'audit	ORG_22	FAU_SAA.1.2
SYS_WEB	40	Le dispositif est accessible par tous	LOG_11	CGS_GDH.1.2

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution