Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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
TOOLS FOR TREATING ISS RISKS

Version 2 - 5 February 2004

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

Document produced by the DCSSI Advisory Office
(SGDN / DCSSI / SDO / BCS)
in collaboration with the EBIOS Club

Comments and suggestions are encouraged and can be sent to the following address:

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
FRANCE

ebios.dcssi@sgdn.pm.gouv.fr

Record of changes

Version	Reason for change	Status
02/1997 (1.1)	Publication of the EBIOS guide	Validated
23/01/2004	Global revision: - Explanations and bringing into line with international security and risk management standards - Highlighting the regulatory baseline within the total set of constraints to be taken into account - Incorporation of the concepts of assumption and security rules (ISO/IEC 15408) - Selected essential elements transferred into the Target system study - Improvement of method for establishing the requirements scale: values representing acceptable limits for the organisation compared with personalised impacts - Incorporation of needs determination for each element in the following activity - Determination of operating mode incorporated into the assumptions - Concepts adapted to ISO/IEC 15408: the source of threats is studied, i.e. the attack methods and the threat agents, together with their characterisation, which may include a type (natural, human, environmental), a cause (accidental, deliberate, detailing in the description available resources, expertise, motivation), an attack potential - Highlighting of attack methods not retained - Formalisation of threats, as understood in ISO/IEC 15408 (threat agents, attack and asset in the form of entities), before comparing with security needs - Comparison of threats with needs modified to allow risks to be identified - Highlighting of non-retained risks - Determination of minimum security objectives incorporated into the activities "Formalisation of security objectives" and "Determination of functional requirements" - Determination of security objectives modified to take into account the assumptions, security policy rules, constraints, regulatory baseline and risks - Determination of security levels added to allow the level of security objectives to be determined (especially in relation to attack potential) and an assurance level to be chosen - Determination of functional security requirements added to allow functional requirements covering security objectives to be determined and the extent of cover presented - Determination of security requirements for assurance added to allow any assurance requirements to be determined Improvements in form, minor adjustments and corrections (grammar, spelling, formulations, presentations, consistency, etc.)	Validated by the EBIOS Club
05/02/2005	Publication of version 2 of the EBIOS guide	Validated

Table of contents

1 Introduction

The EBIOS[1] method comprises five complementary sections.

- Section 1 – Introduction
  This section presents the context, advantages and positioning of the EBIOS approach. It also contains a bibliography, glossary and explanation of acronyms.

- Section 2 – Approach
  This section explains the running of the activities of the method.

- Section 3 – Techniques
  This section proposes means for accomplishing the activities of the method. These techniques will have to be adapted to the organisation's needs and practices.

- Section 4 – Tools for assessing ISS risks
  This section forms the first part of the knowledge bases for the EBIOS method (types of entity, attack methods, vulnerabilities).

- Section 5 – Tools for treating ISS risks
  This section forms the second part of the knowledge bases for the EBIOS method (security objectives, security requirements, tables for determining security functional objectives and requirements).

This document forms the fifth section of the method.

It includes:
- a security objectives base,
- a security requirements base,
- tables used to determine security objectives according to attack methods and vulnerabilities,
- tables used to determine security requirements liable to satisfy security objectives.

[1] EBIOS is a registered trademark of the French General Secretariat of National Defence.

2 Generic security objectives

Security objectives are arranged by entity type and described by a code and name. For the SYS (system) entity type, the security objectives of the other entity types are used.
Although this set of security objectives is certainly not exhaustive, it does cover most ISS themes.
These security objectives must be refined to adapt them to the specific context of the EBIOS study.

2.1 MAT : Hardware

MAT_01	
Content	A stock of emergency equipment must be available in the event of equipment failure
MAT_02	
Content	It must be possible to restore all or part of a system, application, data set and track in the event of damage, failure or negligence
MAT_03	
Content	Moderate changes to the environment (temperature, humidity, air composition) must not result in abnormal behaviour of electronic equipment and media
MAT_04	
Content	Archive media must remain fully readable throughout their storage period
MAT_05	
Content	Equipment and media must be reusable at any time and under any conditions, including exceptional conditions
MAT_06	
Content	There must be a description of all IT equipment and its position
MAT_07	
Content	IT equipment and media (back-up cartridges, hard discs, laptop computers) must be protected against theft
MAT_08	
Content	It must be impossible to reconstruct any sensitive information deleted from a medium
MAT_09	
Content	The equipment must be suitably sized for the services to be provided and must be able to absorb possible periods of overload
MAT_10	
Content	The systems using the equipment must be protected against use by unauthorised persons
MAT_11	
Content	User-friendliness and ease of maintenance must be taken into account when choosing hardware, media and software
MAT_12	
Content	The equipment must comply with hygiene and safety regulations in force in the company
MAT_13	
Content	Supervision and maintenance of the equipment must be provided at all times, including holiday periods, bank holidays and non-working hours

MAT_14	
Content	The equipment must be installed, operated and maintained in guaranteed compliance with the security requirements

MAT_15	
Content	Reliability must be taken into account when choosing equipment, software and media

2.2 LOG : Software

LOG_01	
Content	The integrity of software and data must be guaranteed

LOG_02	
Content	Software updates must not degrade the security or functions of previous versions

LOG_03	
Content	All updating operations on software must be identifiable and justifiable

LOG_04	
Content	The configuration of systems and applications must comply with the security policy requirements

LOG_05	
Content	Any abuse or negligence affecting sensitive applications and the systems accommodating them must be detected

LOG_06	
Content	Before a new tool is put into production its compliance with security policy requirements must be guaranteed

LOG_07	
Content	There must be management of licences and their registration and storage

LOG_08	
Content	The organisation must control the list of configurations installed on its equipment and guarantee their conformity over time

LOG_09	
Content	All software must be installed in compliance with the security requirements and its durability must be guaranteed through maintenance

LOG_10	
Content	It must be possible to analyse operation records, including those generated by other systems (possibility of reconstructing event chains)

LOG_11	
Content	There must be active management of authorisation within the systems, ensuring that information is processed according to the need to know and need to modify

LOG_12	
Content	The use of communication or collaborative work resources that do not comply with the security policy requirements must be subject to special conditions and rules

LOG_13	
Content	All access to the systems must be protected by an authentication and identification device

LOG_14	
Content	System failures or operation beyond system limits must be prevented

LOG_15	

Content	It must be possible to detect abnormal behaviour of any system in real time or retrospectively, trace the operations carried out and identify the authors
LOG_16	
Content	The displaying of sensitive data must not be a security flaw that compromises data confidentiality
LOG_17	
Content	Software must be designed to reduce errors in use

2.3 RES : Network

RES_01	
Content	Access to communication interfaces must be protected against malicious or abusive use
RES_02	
Content	Communication interfaces must protect the confidentiality, integrity and availability of transmissions
RES_03	
Content	It must be possible to establish the authentication and non-repudiation of communications when necessary
RES_04	
Content	Compatibility of the interconnected items must be guaranteed (languages, time zones, standards, etc.)
RES_05	
Content	There must be an updated and clear routing plan
RES_06	
Content	Network accesses must be planned and controlled

2.4 PER : Personnel

PER_01	
Content	Personnel must ensure that equipment and media taken out of the premises are not stolen or broken into.
PER_02	
Content	Personnel with access to sensitive information must be made aware of the risks and identified
PER_03	
Content	Personnel must make correct use of the information tool, communication resources and media and must comply with the security measures applicable according to the classification of the information
PER_04	
Content	There must be a reserve of personnel to guarantee continuity of tasks in the event of absence
PER_05	
Content	The personnel must be committed to the security approach and the roles and responsibilities must be clear and known
PER_06	
Content	New or replacement personnel must be able to perform their tasks in compliance with the security policy
PER_07	

Content	There must be a separation between decision-making, performance and monitoring powers
PER_08	
Content	The personnel must be made accountable and informed of possible sanctions
PER_09	
Content	The personnel must be made aware of the obligation of professional secrecy and discretion
PER_10	
Content	The personnel must be made aware of the organisation's standards and trained to observe with them
PER_11	
Content	The personnel must have the correct reflexes when an incident occurs (duty to inform, means of passing up information, etc.)
PER_12	
Content	The personnel must be trained to use the hardware and software required in their activity
PER_13	
Content	Top management's involvement in the security approach must be real and visible

2.5 PHY : Site

PHY_01	
Content	The supply of services essential to the operation of the equipment (i.e. electricity, communication resources, air-conditioning, etc.) must be guaranteed, of good quality and controlled by the organisation
PHY_02	
Content	The arrangement of the site must prevent observation of confidential information from the outside.
PHY_03	
Content	The site and premises must protect equipment against damage, fires, floods, electromagnetic disturbance, etc.
PHY_04	
Content	Risk limitation must be a factor determining the choice of a site (difficulty of access, flooding, fire, pollution, earthquake, storm, etc.) and the risks must be included in the construction prerequisites
PHY_05	
Content	No compromising electromagnetic signals must be exploitable outside sensitive rooms
PHY_06	
Content	The storage and handling of potentially hazardous materials or equipment must not create risks for the information system
PHY_07	
Content	The site must comply with the organisation's security standards
PHY_08	
Content	Smoking, eating and drinking must be forbidden in rooms housing IT equipment
PHY_09	
Content	Rooms must be protected against the start and spread of fire
PHY_10	

Content	The equipment must be installed and used in compliance with the standards and norms in force (constructor's recommendation, rules of the information system security policy, security standards, etc.)
PHY_11	
Content	Installation of the equipment must be planned and controlled
PHY_12	
Content	The premises and their amenities must be suited to the organisation's missions

2.6 ORG : Organisation

ORG_01	
Content	The organisation must protect the equipment and media against physical access by unauthorised persons
ORG_02	
Content	The entrance and exit procedures must be designed to combat theft of equipment
ORG_03	
Content	The nature and use of transmission resources must guarantee protection of their contents against risks of disclosure, theft, corruption, repudiation and loss
ORG_04	
Content	The organisation must ensure that security policy requirements are observed in the development, use and operation of the systems (hardware and software)
ORG_05	
Content	The restoration policy must guarantee complete recovery of back-ups, including any system changes (hardware, software)
ORG_06	
Content	The anti-virus policy must prevent any malicious code from entering and spreading in the systems
ORG_07	
Content	An archiving policy must guarantee complete recovery of data throughout the period set for their storage
ORG_08	
Content	The organisation must ensure that data (including non-centralised data) are backed up at an adequate frequency
ORG_09	
Content	The organisation must implement a preventive policy against saturation and failure of equipment (IT equipment, air-conditioning, power, communication)
ORG_10	
Content	The organisation must ensure that sufficiently robust passwords are used and correctly managed
ORG_11	
Content	The policy for processing information system records must guarantee compliance with the regulations in force
ORG_12	
Content	The organisation must set up measures to block receipt of unrequested messages (spam) and misinformation using internal communication resources
ORG_13	
Content	The organisation must ensure that solutions are durable by considering the state of the art and the upgrading of the information system

ORG_14	
Content	Each role linked to information system security must always (even in the absence of the holder) be placed under the responsibility of at least one person with the required competencies or able to refer to suitable documentation
ORG_15	
Content	The organisation must check that the level of confidentiality is identified for all information and that suitable rules are applied for its protection
ORG_16	
Content	The organisation must guarantee that emergency resources are operational and that, where possible, they will guarantee continuity of the organisation's sensitive activities in the event of failure, damage or major abuse
ORG_17	
Content	The organisation must ensure that the security instructions are observed in the event of an incident or abuse
ORG_18	
Content	The organisation must guarantee that the minimum security requirements for information systems are observed by everyone
ORG_19	
Content	The organisation must protect the site against the presence of unauthorised persons
ORG_20	
Content	The organisation must check the integrity and authenticity of supplies (hardware, software)
ORG_21	
Content	The organisation must deal with and follow up every security incident identified within it
ORG_22	
Content	The organisation must guarantee that security measures are checked and are an adequate response to the security objectives
ORG_23	
Content	The organisation must check that all rooms comply with the security policy (installation of a technical room or IT room, site access control, surveillance of the premises, fire detection and protection measures, etc.)
ORG_24	
Content	The organisation must guarantee a rapid and effective reaction to a crisis, ensuring that potential impacts are reduced and that essential services continue: failure, damage, major intrusion, other abuse
ORG_25	
Content	The organisation must ensure that work carried out by external operators (service providers, suppliers, etc.) is not a source of risks for the information system
ORG_26	
Content	The organisation must guarantee compliance with the security policy when any sensitive system is installed (hardware or software)
ORG_27	
Content	The organisation must check that all hardware and software is maintained.
ORG_28	
Content	The organisation must check that updated documentation is available for all hardware, software and infrastructures
ORG_29	

Content	The organisation must integrate quality management of its business in compliance with the prevailing standards
ORG_30	
Content	The organisation must protect against unauthorised access to information and data processing
ORG_31	
Content	The organisation of information system security must take the surrounding local context into account (economic, social, political, legislative)
ORG_32	
Content	The organisation must guarantee that security needs and operating constraints are taken into account before and during a development project
ORG_33	
Content	The organisation must limit the possibility of misuse of rights and privileges on the systems
ORG_34	
Content	The organisation must ensure that personnel have access to new technologies (training, partnership, etc.)
ORG_35	
Content	The organisation must ensure that a security policy is implemented to protect and monitor information
ORG_36	
Content	The organisation must ensure that the procedures set up have the flexibility required for their application
ORG_38	
Content	The organisation must ensure that its subcontractors / service providers / suppliers / manufacturers / subsidiaries / other sites comply with the security policy during their operations at the site (work, development, maintenance, etc.)
ORG_37	
Content	The organisation must operate fair sanctions, appropriate to the context, when disregard for the security policy puts information system security in jeopardy
ORG_39	
Content	The organisation must ensure that records and items of proof are used and protected in compliance with the security policy
ORG_40	
Content	The organisation must ensure that all the applicable laws and regulations are taken into account in the security policy
ORG_41	
Content	The organisation must ensure that all applicable rules and procedures are up to date and easily accessible by the persons concerned
ORG_42	
Content	The organisation must ensure that information system management is as straightforward as possible
ORG_43	
Content	Execution of sensitive operations must be checked (operations carried out by more than one person, validation, systematic analysis of records, etc.)
ORG_44	
Content	The accepted residual risks must be analysed in specific studies and if possible an action plan for dealing with an occurrence of the risk must be produced for each residual risk identified

ORG_45	
Content	The organisation must ensure that work conditions are satisfactory

3 Generic functional security requirements

The generic functional security requirements included in this part of the document have been drawn from the following baselines:

- [ISO 15408],
- [ISO 17799],
- various other sources (EBIOS v1, [PSSI], best practices, etc.).

They are arranged by "class", "family" and, if necessary, "sub-family" and described by a code and name.
Although this set of requirements is certainly not exhaustive, it does cover most ISS themes.
These requirements must be refined to adapt them to the specific context of the EBIOS study.

3.1 Requirements taken from ISO 15408

3.1.1 FAU : Security audits

FAU_ARP: Security audit automatic response	
Security alarms	Hierarchical to: no other components. FAU_ARP.1.1 The TSF shall take [assignment: list of the least disruptive actions] upon detection of a potential security violation. Dependencies: FAU_SAA.1 Potential violation analysis Examples Upon detecting a potential security violation, action shall be taken immediately to end the violation and limit its impacts.
FAU_GEN: Security audit data generation	
Audit data generation	Hierarchical to: no other components. FAU_GEN.1.1 The TSF shall be able to generate an audit record for the following auditable events: a) Startup and shutdown of the audit functions; b) All auditable events for the audit level [selection: minimum, basic, detailed, not specified]; c) and [assignment: other specifically defined auditable events]. Dependencies: FPT_STM.1 Reliable time stamps Examples It shall be possible to generate audit records for specified events.
Audit data generation	Hierarchical to: no other components. FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components includedin the PP or ST, [assignment: other audit relevant information] Dependencies: FPT_STM.1 Reliable time stamps Examples

	Audit records shall contain at least the date, time, type of event, subject identity, outcome (success or failure) of the event and any other necessary additional information specified in advance.
Link with user's auditee	Hierarchical to: no other components. FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event. Dependencies: FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification Examples It shall be possible to unambiguously associate each auditable event with the user that caused the event.
FAU_SAA: Security audit analysis	
Analysis of potential violations	Hierarchical to: no other components. FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. Dependencies: FAU_GEN.1 Audit data generation Examples There shall be rules capable of analysing audited events to detect any potential security violations.
Analysis of potential violations	Hierarchical to: no other components. FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation; b) [assignment: any other rules]. Dependencies: FAU_GEN.1 Audit data generation Examples Any auditable events indicating a potential security violation shall be identified accordingly.
Profile-based anomaly detection	Hierarchical to: FAU_SAA.1 FAU_SAA.2.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: the profile target group]. Dependencies: FIA_UID.1 Timing of identification Examples A set of standard system usage profiles representing the historical behaviour patterns of a group of users shall be implemented and kept up to date.
Profile-based anomaly detection	Hierarchical to: FAU_SAA.1 FAU_SAA.2.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent

	with the established patterns of usage represented in the profile. Dependencies: FIA_UID.1 Timing of identification Examples An up-to-date suspicion rating shall be associated with each user with a particular standard usage profile; the index shall indicate the degree to which the user's current activity differs from the established patterns of use represented in the profile.
Profile-based anomaly detection	Hierarchical to: FAU_SAA.1 FAU_SAA.2.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [assignment: conditions under which anomalous activity is reported by the TSF]. Dependencies: FIA_UID.1 Timing of identification Examples Suspicion rating analysis rules shall be implemented to detect potential imminent security policy violations.
Simple attack heuristics	Hierarchical to: FAU_SAA.1 FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [assignment: a subset of system events] that may indicate a violation of the TSP. Dependencies: No dependencies Examples An internal representation of signature events liable to indicate a security policy violation shall be generated and maintained.
Simple attack heuristics	Hierarchical to: FAU_SAA.1 FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: the information to be used to determine system activity]. Dependencies: No dependencies Examples A set of information used to determine the system's activity shall be identified and compared with the signature events liable to indicate a security policy violation.
Simple attack heuristics	Hierarchical to: FAU_SAA.1 FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP. Dependencies: No dependencies Examples Alarm mechanisms shall be implemented to indicate an imminent violation of the security policy when a system event is found to match a signature event that indicates a potential violation.
Complex attack heuristics	Hierarchical to: FAU_SAA.3

	FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the TSP. Dependencies: No dependencies Examples An internal representation of the event sequences of known intrusion scenarios and signature events shall be maintained.
Complex attack heuristics	Hierarchical to: FAU_SAA.3 FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the TSP. Dependencies : No dependencies Examples A set of information used to determine the system's activity shall be identified and compared with the signature events liable to indicate a security policy violation.
Complex attack heuristics	Hierarchical to: FAU_SAA.3 FAU_SAA.4.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP. Dependencies: No dependencies Examples Alarm mechanisms shall be implemented to indicate an imminent violation of the security policy when system events are found to match an event sequence that indicates a potential violation.
FAU_SAR: Security audit review	
Audit review	This component provides authorised users with the capability to obtain and interpret information. Where the users are human, this information needs to be in a human-understandable presentation. Where the users are external IT entities, this information needs to be unambiguously presented in an electronic fashion. Hierarchical to: no other components. FAU_SAR.1.1 The TSF shall provide [assignment: authorised uses] with the capability to read [assignment: list of audit information] from the audit records. Dependencies: FAU_GEN.1 Audit data generation Examples Authorised users shall be able to consult the audit information in audit records.
Audit review	This component provides authorised users with the capability to obtain and interpret information. Where the users are human, this information needs to be in a human-understandable presentation. Where the users are external IT entities, this information needs to be unambiguously presented in an electronic fashion. Hierarchical to: no other components.

	FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information. Dependencies: FAU_GEN.1 Audit data generation Examples Audit records shall be presented in a manner suitable for the user to interpret them.
Restricted audit review	Hierarchical to: no other components. FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read access. Dependencies: FAU_SAR.1 Audit review Examples The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read access.
Selective audit review	Hierarchical to: no other components. FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment: criteria with logical relations]. Dependencies: FAU_SAR.1 Audit review Examples Logically-related criteria in audit data shall be defined such that search, sorting and ordering operations can be performed on the audit data.
FAU_SEL: Security audit event selection	
Selective audit	Hierarchical to: no other components. FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [selection: object identity, user identity, subject identity, host identity, event type] b) [assignment: list of additional attributes that audit selectivity is based upon]. Dependencies: FAU_GEN.1 Audit data generation FMT_MTD.1 TSF data administration Examples It shall be possible to exclude auditable events from the audited event list according to the identity of the object, user, subject or host, the event type or other attributes on which the audit selectivity is based.
FAU_STG: Security audit event storage	
Protected audit trail storage	Hierarchical to: no other components. FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion. Dependencies: FAU_GEN.1 Audit data generation Examples Stored audit records shall be protected against unauthorised deletion.

Protected audit trail storage	Hierarchical to: no other components. FAU_STG.1.2 The TSF shall be able to [selection: prevent, detect] modifications to the audit records. Dependencies: FAU_GEN.1 Audit data generation Examples It shall be possible to detect and/or prevent modifications to audit records.
Guarantees of audit data availability	Hierarchical to: FAU_STG.1 FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion. FAU_STG.2.2 The TSF shall be able to [selection: prevent, detect] modifications to the audit records. FAU_STG.2.3 The TSF shall ensure that [assignment: metric for saving audit records] audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, attack]. Dependencies: FAU_GEN.1 Audit data generation Examples A specified percentage of audit records shall be maintained if the audit data storage capacity is exceeded or in the event of storage failure or attack.
Action in case of possible audit data loss	Hierarchical to: no other components. FAU_STG.3.1 The TSF shall take [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit]. Dependencies: FAU_STG.1 Protected audit trail storage Examples Actions shall be planned in case an audit trail exceeds a pre-defined limit (to be defined).
Prevention of audit data loss	Hierarchical to: FAU_STG.3 FAU_STG.4.1 The TSF shall [selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records'] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full. Dependencies: FAU_STG.1 Protected audit trail storage Examples The measures to be implemented if the maximum audit data storage capacity is reached shall be specified (e.g. ignoring auditable events or overwriting the oldest audit records).

3.1.2 FCO : Communication

FCO_NRO: Non-repudiation of origin	
Selective proof of origin	Hierarchical to: no other components. FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for

	transmitted [assignment: list of information types] at the request of [selection: originator, recipient, [assignment: list of third parties]]. Dependencies: FIA_UID.1 Timing of identification Examples It shall be possible to generate evidence of origin of the transmitted information at the request of the originator, the recipient or third parties, (to be identified).
Selective proof of origin	Hierarchical to: no other components. FCO_NRO.1.2 The TSF shall be able to relate the [assignment: list of attributes] of the originator of the information and the [assignment: list of information fields] of the information to which the evidence applies. Dependencies: FIA_UID.1 Timing of identification Examples It shall be possible to relate the attributes of the originator of the information and the information fields of the information to which the evidence applies.
Selective proof of origin	Hierarchical to: no other components. FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of origin]. Dependencies: FIA_UID.1 Timing of identification Examples The originator, recipient or third parties (to be identified) shall be able to verify the evidence of origin of the information given the limitations on the evidence of origin.
Enforced proof of origin	Hierarchical to: FCO_NRO.1 FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [assignment: list of information types]. FCO_NRO.2.2 The TSF shall be able to relate the [assignment: list of attributes] of the originator of the information and the [assignment: list of information fields] of the information to which the evidence applies. FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of origin]. Dependencies: FIA_UID.1 Timing of identification Examples Evidence of origin shall be generated at all times for certain types of transmitted information (to be identified).
FCO_NRR: Non-repudiation of receipt	
Selective proof of receipt	Hierarchical to: no other components. FCO_NRR.1.1 The TSF shall be able to generate evidence of receipt for received [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]]. Dependencies: FIA_UID.1 Timing of identification

	Examples It shall be possible to generate evidence of receipt of the transmitted information at the request of the originator, the recipient or third parties (to be identified).
Selective proof of receipt	Hierarchical to: no other components. FCO_NRR.1.2 The TSF shall be able to relate the [assignment: list of attributes] of the recipient of the information and the [assignment: list of information fields] of the information to which the evidence applies. Dependencies: FIA_UID.1 Timing of identification Examples It shall be possible to relate the attributes of the recipient of the information and the information fields of the information to which the evidence applies.
Selective proof of receipt	Hierarchical to: no other components. FCO_NRR.1.3 The TSF shall provide a capability to verify the evidence of receipt of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of receipt]. Dependencies: FIA_UID.1 Timing of identification Examples The originator, recipient or third parties (to be identified) shall be able to verify the evidence of receipt of the information given the limitations on the evidence of receipt.
Enforced proof of receipt	Hierarchical to: FCO_NRR.1 FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received [assignment: list of information types]. FCO_NRR.2.2 The TSF shall be able to relate the [assignment: list of attributes] of the recipient of the information and the [assignment: list of information fields] of the information to which the evidence applies. FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of receipt]. Dependencies: FIA_UID.1 Timing of identification Examples Evidence of receipt shall be generated at all times for certain types of transmitted information (to be identified).

3.1.3 FCS : Cryptographic support

FCS_CKM: Cryptographic key management	
Cryptographic key generation	Hierarchical to: no other components. FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key size [assignment: cryptographic key sizes] that met the following: [assignment: list of standards]. Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1

	Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes Examples Cryptographic keys shall be generated in accordance with a specified cryptographic key generation algorithm (to be defined) and specified cryptographic key sizes (to be defined) that comply with the specified standards (to be defined).
Cryptographic key distribution	Hierarchical to: no other components. FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: cryptographic key distribution method] that meets the following: [assignment: list of standards]. Dependencies: [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes Examples Cryptographic keys shall be distributed in accordance with a specified cryptographic key distribution method (to be defined) that complies with the specified standards (to be defined).
Cryptographic key access	Hierarchical to: no other components. FCS_CKM.3.1 The TSF shall perform [assignment: type of cryptographic key access] in accordance with a specified cryptographic key access method [assignment: cryptographic key access method] that meets the following: [assignment: list of standards]. Dependencies: [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes Examples Cryptographic key access types shall be consistent with a specified cryptographic key access method (to be defined) that complies with the specified standards (to be defined).
Cryptographic key destruction	Hierarchical to: no other components. FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards]. Dependencies: [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] FMT_MSA.2 Secure security attributes Examples Cryptographic keys shall be destroyed in accordance with a specified cryptographic key destruction method (to be defined) that complies with the specified standards (to be defined).
FCS_COP: Cryptographic operation	
Cryptographic	Hierarchical to: no other components.

operation	FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]. Dependencies: [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes Examples Cryptographic operations shall be performed in accordance with a specified cryptographic algorithm (to be defined) and key sizes (to be defined) that comply with the specified standards (to be defined).

3.1.4 FDP : User data protection

FDP_ACC: Access control policy	
Subset access control	Hierarchical to: no other components. FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects and operations among subjects and objects covered by the SFP]. Dependencies: FDP_ACF.1 Security attribute based access control Examples With subset access control, the access control security policy shall be enforced on subjects, objects and operations among subjects and objects covered by the specified security policy (to be defined).
Complete access control	Hierarchical to: FDP_ACC.1 FDP_ACC.2.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP. Dependencies: FDP_ACF.1 Security attribute based access control Examples With complete access control, the access control security policy shall be enforced on the specified subjects and objects (to be defined) and all operations among subjects and objects covered by the specified security policy.
Complete access control	Hierarchical to: FDP_ACC.1 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. Dependencies: FDP_ACF.1 Security attribute based access control Examples With complete access control, all operations between any subject and any object in the target scope shall be covered by the access control security policy.
FDP_ACF: Access control functions	
Security attribute based access	Hierarchical to: no other components.

control	FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on [assignment: security attributes, named groups of security attributes]. Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation Examples With security attribute based access control, the access control security policy shall be enforced on objects in accordance with security attributes or security attribute groups (to be defined).
Security attribute based access control	Hierarchical to: no other components. FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]. Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation Examples With security attribute based access control, the rules that govern access to controlled subjects and controlled objects using controlled operations on controlled objects shall always be enforced.
Security attribute based access control	Hierarchical to: no other components. FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]. Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation Examples With security attribute based access control, access of subjects to objects shall be explicitly authorised in accordance with additional rules that explicitly authorise such access (to be defined).
Security attribute based access control	Hierarchical to: no other components. FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]. Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation Examples With security attribute based access control, access of subjects to objects shall be explicitly denied in accordance with additional rules that explicitly deny such access (to be defined).
FDP_DAU: Data authentication	
Basic data authentication	Hierarchical to: no other components. FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or information types].

	Dependencies: No dependencies Examples Specified subjects (to be defined) shall be able to verify evidence of the validity of the indicated information (to be defined).
Basic data authentication	Hierarchical to: no other components. FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or information types]. Dependencies: No dependencies Examples It shall be possible to generate evidence that can be used as a guarantee of the validity of objects or information types (to be defined).
Data authentication with identity of guarantor	Hierarchical to: FDP_DAU.1 FDP_DAU.2.2 The TSF shall provide [assignment: list of subjects] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence. Dependencies: FIA_UID.1 Timing of identification Examples With authentication with identity of guarantor, specified subjects (to be defined) shall have the ability to verify evidence of the validity of the indicated information (to be defined) and the identity of the user that generated the evidence.
FDP_ETC: Export to outside TSF control	
Export of user data without security attributes	Hierarchical to: no other components. FDP_ETC.1.1 The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TSC. FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes. Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Examples When data is exported without security attributes, user data shall be exported without the user data's associated security attributes.
Export of user data without security attributes	Hierarchical to: no other components. FDP_ETC.1.1 The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TSC. FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes. Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Examples

	When data is exported without security attributes, user data shall be exported without the user data's associated security attributes.
Export of user data with security attributes	Hierarchical to: no other components. FDP_ETC.2.1 The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TSC. FDP_ETC.2.2 The TSF shall export the user data with its associated security attributes. Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Examples When data is exported with security attributes, user data shall be exported with its associated security attributes.
Export of user data with security attributes	Hierarchical to: no other components. FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data. Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Examples When user data is exported, its security attributes shall be unambiguously associated with it.
Export of user data with security attributes	Hierarchical to: no other components. FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC [assignment: additional exportation control rules]. Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] Examples The additional exportation control rules (to be defined) shall be enforced when exporting user data outside the security domain.
FDP_IFC: Information flow control policy	
Subset information flow control	Hierarchical to: no other components. FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]. Dependencies: FDP_IFF.1 Simple security attributes Examples For a subset information flow control, the security policy must be applied to subjects, information, and operations that cause the transfer to and from controlled subjects
Complete information flow	Hierarchical to: FDP_IFC.1

control	FDP_IFC.2.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP. Dependencies: FDP_IFF.1 Simple security attributes Examples For a complete information flow control, the security policy for information flow control must be applied to subjects, information and all operations that cause the transfer to and from controlled subjects
Complete information flow control	Hierarchical to: FDP_IFC.1FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP. Dependencies: FDP_IFF.1 Simple security attributes Examples For a complete information flow control, all operations that cause the transfer of information to and from all subjects of a security area must be covered by a flow control security policy
FDP_IFF: Information flow control functions	
Simple security attributes	Hierarchical to: no other components. FDP_IFF.1.1 The TSF shall enforce the [assignment: assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. Dependencies: FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation Examples For simple security attributes, an information flow between a controlled subject and controlled information via a controlled operation must be authorized in function to rules based upon the security attributes (to be defined)
Simple security attributes	Hierarchical to: no other components. FDP_IFF.1.1 The TSF shall enforce the [assignment: assignment: information

	flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. Dependencies: FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation Examples The security policy for flow control must be applied in function to a minimum number of identified security attributes (to be defined)
Simple security attributes	Hierarchical to: no other components. FDP_IFF.1.1 The TSF shall enforce the [assignment: assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. Dependencies: FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation Examples The additional security policy rules for flow control (to be defined) must be applied
Simple security	Hierarchical to: no other components.

attributes	FDP_IFF.1.1 The TSF shall enforce the [assignment: assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. Dependencies: FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation Examples A list of additional security policy capabilities (to be defined) must be provided
Simple security attributes	Hierarchical to: no other components. FDP_IFF.1.1 The TSF shall enforce the [assignment: assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. Dependencies: FDP_IFC.1 Subset information flow controlFMT_MSA.3 Static attribute initialisation Examples An information flow must be explicitly authorized in function to rules based on security attributes that explicitly authorize information flows (to be defined)

Simple security attributes	Hierarchical to: no other components. FDP_IFF.1.1 The TSF shall enforce the [assignment: assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. Dependencies: FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation Examples An information flow must be explicitly denied in function to rules based on security attributes that explicitly deny information flows (to be defined)
Hierarchical security attributes	Hierarchical to: FDP_IFF.1 FDP_IFF.2.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.2.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.2.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.2.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes: a) there exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater

	than the other, or if the security attributes are incomparable; and b) there exist 'pairwise upper bounds' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and c) there exist "pairwise lower bounds" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute for which both of the two original valid security attributes are greater than the security attribute. Dependencies: FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation Examples For hierarchical security attributes, an information flow between a subject and controlled information via a controlled operation must be authorized according to rules based on the ordering relationships between security attributes (to be defined)
Hierarchical security attributes	Hierarchical to: FDP_IFF.1 FDP_IFF.2.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.2.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.2.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.2.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes: a) there exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and b) there exist 'pairwise upper bounds' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and c) there exist "pairwise lower bounds" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute for which both of the two original valid security attributes are greater than the security attribute. Dependencies: FDP_IFC.1 Subset information flow controlFMT_MSA.3 Static attribute initialisation Examples

	For hierarchical security attributes, there must exist an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one is greater than the other, or if they are incomparable
Hierarchical security attributes	Hierarchical to: FDP_IFF.1 FDP_IFF.2.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]. FDP_IFF.2.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.2.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.2.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes: a) there exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and b) there exist 'pairwise upper bounds' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and c) there exist "pairwise lower bounds" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute for which both of the two original valid security attributes are greater than the security attribute. Dependencies: FDP_IFC.1 Subset information flow controlFMT_MSA.3 Static attribute initialisation Examples For hierarchical security attributes, there must exist 'pairwise upper bounds', such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes
Hierarchical security attributes	Hierarchical to: FDP_IFF.1 FDP_IFF.2.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes]. FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

	FDP_IFF.2.3 The TSF shall enforce the [assignment: additional information flow control SFP rules]. FDP_IFF.2.4 The TSF shall provide the following [assignment: list of additional SFP capabilities]. FDP_IFF.2.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows]. FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes: a) there exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and b) there exist 'pairwise upper bounds' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and c) there exist "pairwise lower bounds" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute for which both of the two original valid security attributes are greater than the security attribute. Dependencies: FDP_IFC.1 Subset information flow controlFMT_MSA.3 Static attribute initialisation Examples For hierarchical security attributes, there must exist a "pairwise lower bounds", such that, given any two valid security attributes, there is a valid security attribute for which both of the two original valid security attributes are greater than the security attribute
Limited illicit information flows	Hierarchical to: no other components. FDP_IFF.3.1 The TSF shall enforce the [assignment: information flow control SFP] to limit the capacity of [assignment: types of illicit information flows] to a [assignment: maximum capacity]. Dependencies: AVA_CCA.1 Covert channel analysis FDP_IFC.1 Subset information flow control Examples Enforcement of the security policy for flow control must enable limiting the types of illicit information flows (to be defined) to a maximum capacity (to be defined)
Partial elimination of illicit information flows	Hierarchical to: FDP_IFF.3 FDP_IFF.4.1 The TSF shall enforce the [assignment: information flow control SFP] to limit the capacity of [assignment: types of illicit information flows] to a [assignment: maximum capacity]. FDP_IFF.4.2 The TSF shall prevent [assignment: types of illicit information flows]. Dependencies: AVA_CCA.1 Covert channel analysis FDP_IFC.1 Subset information flow control Examples

	For a partial elimination of illicit information flow, enforcement of the security policy for flow control must prevent certain types of identified illicit flows (to be defined)
No illicit information flows	Hierarchical to: FDP_IFF.4 FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [assignment: name of information flow control SFP]. Dependencies: AVA_CCA.3 Exhaustive covert channel analysis FDP_IFC.1 Subset information flow control Examples For complete elimination of illicit information flow, enforcement of the security policy for flow control must guarantee that no illicit information flow exists to bypass flow control measures
Illicit information flow monitoring	Hierarchical to: no other components. FDP_IFF.6.1 The TSF shall enforce the [assignment: information flow control SFP] to monitor [assignment: types of illicit information flows] when it exceeds the [assignment: maximum capacity]. Dependencies: AVA_CCA.1 Covert channel analysis FDP_IFC.1 Subset information flow control Examples The security policy for flow control must permit monitoring illicit flow types (to define) when they exceed a maximum capacity (to be defined)
FDP_ITC: Import from outside TSF control	
Import of user data without security attributes	Hierarchical to: no other components. FDP_ITC.1.1The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation Examples For an import without security attributes, all user data security attributes must be ignored when importing user data from outside
Import of user data without security attributes	Hierarchical to: no other components. FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: additional importation control rules]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation Examples The additional importation control rules of the security policy must be enforced (to be defined)

Import of user data without security attributes	Hierarchical to: no other components. FDP_ITC.1.1 The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation Examples The security policy for access control or for flow control must be enforced when importing data from outside the security domain
Import of user data with security attributes	Hierarchical to: no other components. FDP_ITC.2.1 The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data. FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: additional importation control rules]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency Examples For an import with security attributes, the security attributes associated with imported user data must be used
Import of user data with security attributes	Hierarchical to: no other components. FDP_ITC.2.1 The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

	FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: additional importation control rules]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency Examples For an import with security attributes, the protocol used must provide for the unambiguous association between the security attributes and the user data received
Import of user data with security attributes	Hierarchical to: no other components. FDP_ITC.2.1 The TSF shall enforce the [assignment: access control SFP and/or information flow control SFP] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data. FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: additional importation control rules]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency Examples For an import with security attributes, the interpretation of the security attributes of the imported user data must be as intended by the source of the user data
FDP_ITT: Internal TOE transfer	
Basic internal transfer protection	Hierarchical to: no other components. FDP_ITT.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] Examples The security policy for access control or information flow control must prevent disclosure, modification or loss of user data when it is transmitted between physically-separated parts of the security domain
Transmission separation by	Hierarchical to: FDP_ITT.1

attributes	FDP_ITT.2.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE. FDP_ITT.2.2 The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following: [assignment: security attributes that require separation]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] Examples For a Transmission separation by attribute, controlled data transmitted between physically-separated parts of the security domain must be separated in function to security attributes that require attribute separation
Integrity monitoring	Hierarchical to: no other components. FDP_ITT.3.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors]. FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken upon integrity error]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_ITT.1 Basic internal transfer protection Examples Integrity errors must be detected during transmission of user data between physically-separated parts of the security domain
Integrity monitoring	Hierarchical to: no other components. FDP_ITT.3.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors]. FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken upon integrity error]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_ITT.1 Basic internal transfer protection Examples Upon detection of a data integrity error, specific actions (to be defined) must be taken
Attribute-based integrity monitoring	Hierarchical to: FDP_ITT.3 FDP_ITT.4.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors], based on the following attributes: [assignment: security attributes that require separate transmission channels].FDP_ITT.4.2 Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken

	upon integrity error].Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]FDP_ITT.2 Transmission separation by attributeExamplesFDP_ITT.3.1: Attribute-based integrity monitoring which requires separate transmission channels. Hierarchical to: FDP_ITT.3 FDP_ITT.4.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors], based on the following attributes: [assignment: security attributes that require separate transmission channels]. FDP_ITT.4.2 Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken upon integrity error]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_ITT.2 Transmission separation by attribute Examples FDP_ITT.3.1: Attribute-based integrity monitoring which requires separate transmission channels.
FDP_RIP: Residual information protection	
Subset residual information protection	Hierarchical to: no other components. FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects]. Dependencies: No dependencies Examples For a subset residual information protection, any previous information content of a resource must be made unavailable upon the allocation or the deallocation of the resource from objects (to be defined)
Full residual information protection	FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] all objects. Dependencies: No dependencies Examples For full residual information protection, any previous information content of a resource must be made unavailable upon the allocation or the deallocation of the resource from all objects
FDP_ROL: Rollback	
Basic rollback	Hierarchical to: no other components. FDP_ROL.1.1 The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] to permit the rollback of the [assignment: list of operations] on the [assignment: list of objects]. FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [assignment: boundary limit to which rollback may be performed]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset

	information flow control] Examples For basic rollback, rollback of operations (to be defined) on the identified objects (to define) must be permitted
Basic rollback	Hierarchical to: no other components. FDP_ROL.1.1 The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] to permit the rollback of the [assignment: list of operations] on the [assignment: list of objects]. FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [assignment: boundary limit to which rollback may be performed]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] Examples For basic rollback, rollback of operations must be permitted within the boundary limit to which rollback may be performed (to be defined)
Advanced rollback	Hierarchical to: FDP_ROL.1 FDP_ROL.2.1 The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] to permit the rollback of all the operations on the [assignment: list of objects]. FDP_ROL.2.2 The TSF shall permit operations to be rolled back within the [assignment: boundary limit to which rollback may be performed]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] Examples For advanced rollback, rollback of all operations on the identified objects (to be defined) must be possible
FDP_SDI: Stored data integrity	
Stored data integrity monitoring	Hierarchical to: no other components. FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes]. Dependencies: No dependencies Examples Stored user data must be monitored for integrity errors on all objects in function to user data attributes (to be defined)
Stored data integrity monitoring and action	Hierarchical to: FDP_SDI.1 FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes]. FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: action to be taken]. Dependencies: No dependencies

	Examples Upon detection of a data integrity error, specific actions (to be defined) must be taken
FDP_UCT: Inter-TSF user data confidentiality transfer protection	
Basic data exchange confidentiality	Hierarchical to: no other components. FDP_UCT.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to [selection: transmit, receive] objects in a manner protected from unauthorized disclosure. Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] Examples Objects must be transmitted and received in a manner protected from unauthorized disclosure
FDP_UIT: Inter-TSF user data integrity transfer protection	
Data exchange integrity	Hierarchical to: no other components. FDP_UIT.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to [selection: transmit, receive] user data in a manner protected from errors of [selection: modification, deletion, insertion, replay]. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] Examples User data must be transmitted and received in a manner protected from modification, deletion, insertion or replay
Data exchange integrity	Hierarchical to: no other components. FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection: modification, deletion, insertion, replay] has occurred. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] Examples Upon reception of user data, it must be possible to determine if modification, deletion, insertion or replay has occurred
Source data exchange recovery	Hierarchical to: no other components. FDP_UIT.2.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to recover from [assignment: list of recoverable errors] with the help of the source trusted IT product. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_UIT.1 Data exchange integrity

	FTP_ITC.1 Inter-TSF trusted channel Examples For source data exchange recovery, the data must be recoverable, for errors compatible with the list of recoverable errors (to be defined), with the help of the source trusted IT product.
Destination data exchange recovery	Hierarchical to: FDP_UIT.2 FDP_UIT.3.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to recover from [assignment: list of recoverable errors] without any help from the source trusted IT product. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]FDP_UIT.1 Data exchange integrity FTP_ITC.1 Inter-TSF trusted channel Examples For destination data exchange recovery, the data must be recoverable, for recoverable errors (to be defined) without any help from the source trusted IT product.

3.1.5 FIA : Identification and authentication

FIA_AFL: Authentication failures	
Authentication failure handling	Hierarchical to: no other components. FIA_AFL.1.1 The TSF shall detect when [assignment: number] unsuccessful authentication attempts occur related to [assignment: list of authentication events]. Dependencies: FIA_UAU.1 Timing of authentication Examples The system shall detect when a number (to define) of unsuccessful authentication attempts occur related to authentication events (to be defined)
Authentication failure handling	Hierarchical to: no other components. FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions]. Dependencies: FIA_UAU.1 Timing of authentication Examples Specific actions (to define) must be taken when the defined number of unsuccessful authentication attempts has been met or surpassed
FIA_ATD: User attribute definition	
User attribute definition	Hierarchical to: no other components. FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: [assignment: list of security attributes]. Dependencies: No dependencies Examples A list of security attributes belonging to individual users must be maintained (to

	be defined)
FIA_SOS: Specification of secrets	
Verification of secrets	Hierarchical to: no other components. FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric]. Dependencies: No dependencies Examples A mechanism must verify that secrets meet a defined quality metric (to be defined)
TSF Generation of secrets	Hierarchical to: no other components. FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [assignment: a defined quality metric]. Dependencies: No dependencies Examples A mechanism must be provided to generate secrets that meet a defined quality metric (to be defined)
TSF Generation of secrets	Hierarchical to: no other components. FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions]. Dependencies: No dependencies Examples The use of secrets generated in a FIA_SOS.2.1 context must be made obligatory for identified functions (to be defined)
FIA_UAU: User authentication	
Timing of authentication	Hierarchical to: no other components. FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated. Dependencies: FIA_UID.1 Timing of identification Examples Certain actions passing through the system on behalf of the user (to be defined) must be permitted before the user is authenticated
Timing of authentication	Hierarchical to: no other components. FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. Dependencies: FIA_UID.1 Timing of identification Examples Each user must be successfully authenticated before allowing any actions passing through the system on behalf of the user excepting actions defined by FIA_UAU.1.1

Unforgeable authentication	Hierarchical to: no other components. FIA_UAU.3.1 The TSF shall [selection: detect, prevent] use of authentication data that has been forged by any user of the TSF. Dependencies: No dependencies Examples Use of authentication data that has been forged by any kind of user must be detected and prevented
Unforgeable authentication	Hierarchical to: no other components. FIA_UAU.3.2 The TSF shall [selection: detect, prevent] use of authentication data that has been copied from any other user of the TSF. Dependencies: No dependencies Examples Use of authentication data copied from any user other than the official user must be detected and prevented
Single-use authentication mechanisms	Hierarchical to: no other components. FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)]. Dependencies: No dependencies Examples For a single-use authentication, reuse of authentication data related to identified authentication mechanisms (to define) must be prevented
Multiple authentication mechanisms	Hierarchical to: no other components. FIA_UAU.5.1 The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication. Dependencies: No dependencies Examples For multiple authentication mechanisms, multiple authentication mechanisms (to define) must be provided to support user authentication
Multiple authentication mechanisms	Hierarchical to: no other components. FIA_UAU.5.2 The TSF shall authenticate any user’s claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication]. Dependencies: No dependencies Examples For multiple authentication mechanisms, the user's claimed identity must be authenticated according to the rules describing how the multiple authentication mechanisms provide authentication (to be defined)
Re-authenticating	Hierarchical to: no other components.

	FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: list of conditions under which re-authentication is required]. Dependencies: No dependencies Examples The user must be re-authenticated under the specific conditions under which re-authentication is required (to be defined)
Protected authentication feedback	Hierarchical to: no other components. FIA_UAU.7.1 The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress. Dependencies: FIA_UAU.1 Timing of authentication Examples Only certain specific information (to be defined) can be provided to the user while the authentication is in progress.
FIA_UID : User identification	
Timing of identification	Hierarchical to: no other components. FIA_UID.1.1 The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified. Dependencies: No dependencies Examples Certain actions passing through the system on behalf of the user (to define) must be authorized before the user is identified.
Timing of identification	Hierarchical to: no other components. FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. Dependencies: No dependencies Examples Each user must be successfully identified before authorizing any actions passing through the system on behalf of the user excepting actions defined by FIA_UAU.1.1
FIA_USB: User-subject binding	
User-subject binding	Hierarchical to: no other components. FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user. Dependencies: FIA_ATD.1 User attribute definition Examples The appropriate user security attributes must be associated with subjects acting on behalf of that user

3.1.6 FMT : Security management

FMT_MOF: Management of functions in TSF

Management of security functions behaviour	Hierarchical to: no other components. FMT_MOF.1.1 The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorized identified roles]. Dependencies: FMT_SMR.1 Security roles Examples The ability to determine the behaviour of or to disable, enable, modify the behaviour of identified functions (to be defined) must be restricted to the authorized identified roles (to be defined)
FMT_MSA: Management of security attributes	
Management of security attributes	Hierarchical to: no other components. FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles]. Dependencies: FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles Examples The ability to change the default value, to query, to modify, to delete and to perform other identified operations (to be defined) for certain security attributes (to be defined) must be restricted to the authorized identified roles (to be defined)
Secure security attributes	Hierarchical to: no other components.FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes Dependencies: ADV_SPM.1 Informal TOE security policy model FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles Examples Only secure values shall be accepted for security attributes
Static attribute initialisation	Hierarchical to: no other components. FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection: restrictive, permissive, other property] default values for security attributes that are used to enforce the SFP. Dependencies: FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles Examples Restrictive, permissive or other property (to be defined) default values for security attributes that are used to enforce the security policy must be provided
Static attribute initialisation	Hierarchical to: no other components. FMT_MSA.3.2 The TSF shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.

	Dependencies: FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles Examples The authorized identified roles (to be defined) must be able to specify alternative initial values to override the default values when an object or information is created
FMT_MTD: Management of TSF data	
Management of TSF data	Hierarchical to: no other components. FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles]. Dependencies: FMT_SMR.1 Security roles Examples The ability to change the default value, to query, to modify, to delete and to perform other identified operations (to define) for certain identified data (to define) must be restricted to the authorized roles (to be defined)
Management of TSF data	Hierarchical to: no other components. FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment: list of TSF data] to [assignment: the authorized identified roles]. Dependencies: FMT_MTD.1 Management of TSF data FMT_SMR.1 Security roles Examples The specification of the limits for certain data (to be defined) must be restricted to the authorized identified roles (to be defined)
Management of TSF data	Hierarchical to: no other components. FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: actions to be taken]. Dependencies: FMT_MTD.1 Management of TSF data FMT_SMR.1 Security roles Examples Specific actions (to be defined) must be taken if the data are at the limits indicated by FMT_MTD.2.2, or exceed them
Secure TSF data	Hierarchical to: no other components. FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data. Dependencies: ADV_SPM.1 Informal TOE security policy model FMT_MTD.1 Management of TSF data Examples Only secure values shall be accepted for system data
FMT_REV: Revocation	
Revocation	Hierarchical to: no other components.

	FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [selection: users, subjects, objects, other additional resources] within the TSC to [assignment: the authorized identified roles]. Dependencies: FMT_SMR.1 Security roles Examples Only the authorized identified roles (to be defined) shall have the ability to revoke security attributes associated with users, subjects, objects and other additional resources (to be defined) within the system
Revocation	Hierarchical to: no other components. FMT_REV.1.2 The TSF shall enforce the rules [assignment: specification of revocation rules]. Dependencies: FMT_SMR.1 Security roles Examples Specific revocation rules (to be defined) must be implemented
FMT_SAE: Security attribute expiration	
Time-limited authorisation	Hierarchical to: no other components. FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [assignment: list of security attributes for which expiration is to be supported] to [assignment: the authorized identified roles]. Dependencies: FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps Examples Only the authorized identified roles (to be defined) shall have the capability to specify an expiration time for certain security attributes for which an expiration date is to be supported (to be defined)
Time-limited authorisation	Hierarchical to: no other components. FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: list of actions to be taken for each security attribute] after the expiration time for the indicated security attribute has passed. Dependencies: FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps Examples Certain specific actions (to be defined) for each attribute identified by FMT_SAE.1.1) must be able to be taken after the expiration time for the indicated security attribute has passed
FMT_SMR: Security management roles	
Security roles	Hierarchical to: no other components. FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorized identified roles]. FMT_SMR.1.2 The TSF shall be able to associate users with roles. Dependencies: FIA_UID.1 Timing of identification Examples

	The authorized identified roles (to be defined) must be maintained
Security roles	Hierarchical to: no other components. FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorized identified roles]. FMT_SMR.1.2 The TSF shall be able to associate users with roles. Dependencies: FIA_UID.1 Timing of identification Examples It must be possible to associate users with roles.
Restrictions on security roles	Hierarchical to: FMT_SMR.1 FMT_SMR.2.1 The TSF shall maintain the roles: [assignment: the authorized identified roles]. FMT_SMR.2.2 The TSF shall be able to associate users with roles. FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: conditions for the different roles] are satisfied. Dependencies: FIA_UID.1 Timing of identification Examples For restrictions on security roles, the conditions for the different roles must be satisfied
Assuming roles	Hierarchical to: no other components. FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: [assignment: the roles]. Dependencies: FMT_SMR.1 Security roles Examples The assumption of certain identified roles (to be defined) shall require an explicit request

3.1.7 FPR : Privacy

FPR_ANO: Anonymity	
Anonymity	Hierarchical to: no other components. FPR_ANO.1.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects]. Dependencies: No dependencies Examples Sets of users and/or subjects (to be defined) must be unable to determine the real user name bound to subjects and/or operations and/or identified objects (to be defined)
Anonymity without soliciting information	Hierarchical to: FPR_ANO.1 FPR_ANO.2.1 The TSF shall ensure that [assignment: set of users and/or

	subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects]. FPR_ANO.2.2 The TSF shall provide [assignment: list of services] to [assignment: list of subjects] without soliciting any reference to the real user name. Dependencies: No dependencies Examples For anonymity without soliciting information , certain services (to be defined) must be provided certain subjects (to be defined) without soliciting any reference to the real user name
FPR_PSE: Pseudonymity	
Pseudonymity	Hierarchical to: no other components. FPR_PSE.1.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects]. FPR_PSE.1.2 The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects]. FPR_PSE.1.3 The TSF shall [selection: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric]. Dependencies: No dependencies Examples Sets of users and/or subjects (to be defined) must be unable to determine the real user name bound to subjects and/or operations and/or identified objects (to be defined)
Pseudonymity	Hierarchical to: no other components. FPR_PSE.1.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects]. FPR_PSE.1.2 The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects]. FPR_PSE.1.3 The TSF shall [selection: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric]. Dependencies: No dependencies Examples It must be possible to provide a certain number of aliases (to define) for the real user name bound to identified subjects (to be defined)
Pseudonymity	Hierarchical to: no other components. FPR_PSE.1.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects] FPR_PSE.1.2 The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects].

	FPR_PSE.1.3 The TSF shall [selection: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric]. Dependencies: No dependencies Examples The system must determine an alias for a user, accept the alias of the user and control that the alias conforms to the alias metric (to be defined)
Reversible pseudonymity	Hierarchical to: FPR_PSE.1 FPR_PSE.2.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects]. FPR_PSE.2.2 The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects]. FPR_PSE.2.3 The TSF shall [selection: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric]. FPR_PSE.2.4 The TSF shall provide [selection: an authorized user, [assignment: list of trusted subjects]] a capability to determine the user identity based on the provided alias only under the following [assignment: list of conditions]. Dependencies: FIA_UID.1 Timing of identification Examples For reversible pseudonymity, authorized users and trusted subjects (to be defined) shall be able to determine the user identity based on the provided alias only under certain conditions (to be defined)
Alias pseudonymity	Hierarchical to: FPR_PSE.1 FPR_PSE.3.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects]. FPR_PSE.3.2 The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects]. FPR_PSE.3.3 The TSF shall [selection: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric]. FPR_PSE.3.4 The TSF shall provide an alias to the real user name which shall be identical to an alias provided previously under the following [assignment: list of conditions] otherwise the alias provided shall be unrelated to previously provided aliases. Dependencies: No dependencies Examples For alias pseudonymity, the alias to the real user name must be identical to an alias provided previously under certain conditions (to be defined)
Alias pseudonymity	Hierarchical to: FPR_PSE.1 FPR_PSE.3.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].

	FPR_PSE.3.2 The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects]. FPR_PSE.3.3 The TSF shall [selection: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric]. FPR_PSE.3.4 The TSF shall provide an alias to the real user name which shall be identical to an alias provided previously under the following [assignment: list of conditions] otherwise the alias provided shall be unrelated to previously provided aliases. Dependencies: No dependencies Examples For alias pseudonymity, if FPR_PSE.3.4.1 cannot be respected, the alias provided must be unrelated with aliases provided previously
FPR_UNL: Unlinkability	
Unlinkability	Hierarchical to: no other components. FPR_UNL.1.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine whether [assignment: list of operations] [selection: were caused by the same user, are related as follows [assignment: list of relations]]. Dependencies: No dependencies Examples Sets of users and/or subjects (to be defined) must be unable to determine whether certain relationships (to be defined) were caused by the same user or are related according to identified relationships (to be defined)
FPR_UNO: Unobservability	
Unobservability	Hierarchical to: no other components. FPR_UNO.1.1 The TSF shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects]. Dependencies: No dependencies Examples Users and identified subjects (to be defined) must be unable to observe the operation of certain operations (to be defined) on objects (to be defined) by certain protected users and subjects (to be defined)
Allocation of information impacting unobservability	Hierarchical to: FPR_UNO.1 FPR_UNO.2.1 The TSF shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].

	FPR_UNO.2.2 The TSF shall allocate the [assignment: unobservability related information] among different parts of the TOE such that the following conditions hold during the lifetime of the information: [assignment: list of conditions]. Dependencies: No dependencies Examples For an allocation of information impacting unobservability, unobservability related information (to be defined) must be allocated among different parts of the system such that certain conditions hold (to be defined)
Unobservability without soliciting information	Hierarchical to: no other components. FPR_UNO.3.1 The TSF shall provide [assignment: list of services] to [assignment: list of subjects] without soliciting any reference to [assignment: privacy related information]. Dependencies: FPR_UNO.1 Unobservability Examples Certain services (to be defined) must be provided identified subjects (to be defined) without soliciting any reference to privacy related information (to be defined)
Authorized user observability	Hierarchical to: no other components. FPR_UNO.4.1 The TSF shall provide [assignment: set of authorized users] with the capability to observe the usage of [assignment: list of resources and/or services]. Dependencies: No dependencies Examples Authorized users (to be defined) must have the capability to observe the usage of identified resources and/or services (to be defined)

3.1.8 FPT : Protection of the TSF

FPT_AMT: Underlying abstract machine test	
Abstract machine testing	Hierarchical to: no other components. FPT_AMT.1.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorized user, other conditions] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. Dependencies: No dependencies Examples Tests must be run during initial start-up to demonstrate the correct operation of the security assumptions provided by the systems responsible for security
Abstract machine testing	Hierarchical to: no other components. FPT_AMT.1.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorized user, other conditions] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. Dependencies: No dependencies

	Examples Tests must be run during normal operation to demonstrate the correct operation of the security assumptions provided by the systems responsible for security
Abstract machine testing	Hierarchical to: no other components. FPT_AMT.1.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorized user, other conditions] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. Dependencies: No dependencies Examples Tests must be run at the request of an authorized user to demonstrate the correct operation of the security assumptions provided by the systems responsible for security
Abstract machine testing	Hierarchical to: no other components.FPT_AMT.1.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorized user, other conditions] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. Dependencies: No dependencies Examples Tests must be run in certain complementary conditions (to define) to demonstrate the correct operation of the security assumptions provided by the systems responsible for security
FPT_FLS: Fail secure	
Failure with preservation of secure state	Hierarchical to: no other components. FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF]. Dependencies: ADV_SPM.1 Informal TOE security policy model Examples The systems responsible for security must preserve a secure state when some types (to be defined) of failures occur
FPT_ITA : Availability of exported TSF data	
Inter-TSF availability within a defined availability metric	Hierarchical to: no other components. FPT_ITA.1.1 The TSF shall ensure the availability of [assignment: [assignment: list of types of TSF data] provided to a remote trusted IT product within [assignment: a defined availability metric] given the following conditions [assignment: conditions to ensure availability]. Dependencies: No dependencies Examples The availability of certain security data (to be defined) provided to a remote trusted IT product within a defined availability metric (to be defined) given conditions (to be defined) to ensure availability[GRL1]
FPT_ITC: Confidentiality of exported TSF data	

Inter-TSF confidentiality during transmission	Hierarchical to: no other components. FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission. Dependencies: No dependencies Examples All security data transmitted from a system responsible for security to a remote trusted IT product must be protected from unauthorized disclosure during their transmission
FPT_ITI: Integrity of exported TSF data	
Détection d'une modification inter-TSF	Hierarchical to: no other components. FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: a defined modification metric]. FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: action to be taken] if modifications are detected. Dependencies: No dependencies Examples Any modification of security data during transmission between a system responsible for security and a remote trusted IT product must be detected within the limits of a specific modification metric (to be defined)
Inter-TSF detection of modification	Hierarchical to: no other components. FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: a defined modification metric]. FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: action to be taken] if modifications are detected. Dependencies: No dependencies Examples The integrity of all security data transmitted between a system responsible for security and a remote trusted IT product must be controlled and actions (to be defined) must be taken if modifications are detected
Inter-TSF detection and correction of modification	Hierarchical to: FPT_ITI.1 FPT_ITI.2.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: a defined modification metric]. FPT_ITI.2.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: action to be taken] if modifications are detected. FPT_ITI.2.3 The TSF shall provide the capability to correct [assignment: type of modification] of all TSF data transmitted between the TSF and a remote trusted IT product. Dependencies: No dependencies Examples For inter-system detection of a modification, the types of modification (to be

	defined) of all security data transmitted between a system responsible for security and a remote trusted IT product must be able to be corrected
FPT_ITT: Internal TOE TSF data transfer	
Basic internal TSF data transfer protection	Hierarchical to: no other components. FPT_ITT.1.1 The TSF shall protect TSF data from[selection: disclosure, modification] when it is transmitted between separate parts of the TOE. Dependencies: No dependencies Examples Security data must be protected from disclosure and modification when it is transmitted between separate parts of the system
TSF data transfer separation	Hierarchical to: FPT_ITT.1 FPT_ITT.2.1 The TSF shall protect TSF data from [selection: disclosure, modification] when it is transmitted between separate parts of the TOE. FPT_ITT.2.2 The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE. Dependencies: No dependencies Examples User data must be separated from security data when such data is transmitted between separate parts of the system
TSF data integrity monitoring	Hierarchical to: no other components. FPT_ITT.3.1 The TSF shall be able to detect [selection: modification of data, substitution of data, re-ordering of data, deletion of data, [assignment: other integrity errors]] for TSF data transmitted between separate parts of the TOE. Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection Examples Modification, substitution, re-ordering, deletion, or other integrity errors (to be defined) affecting security data transmitted between separate parts of the system must be detected
TSF data integrity monitoring	Hierarchical to: no other components. FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: specify the action to be taken]. Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection Examples Specific actions (to be defined) must be taken upon detection of a data integrity error
FPT_PHP: TSF physical protection	
Passive detection of physical attack	Hierarchical to: no other components. FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. Dependencies: FMT_MOF.1 Management of security functions behaviour

	Examples Any physical tampering that might compromise system security must be detected in an unambiguous manner
Passive detection of physical attack	Hierarchical to: no other components. FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. Dependencies: FMT_MOF.1 Management of security functions behaviour Examples It must be possible to determine if physical tampering with security devices or with security elements has occurred
Notification of physical attack	Hierarchical to: FPT_PHP.1FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. FPT_PHP.2.3 For [assignment: list of TSF devices/elements for which active detection is required], the TSF shall monitor the devices and elements and notify [assignment: a designated user or role] when physical tampering with the TSF's devices or TSF's elements has occurred. Dependencies: FMT_MOF.1 Management of security functions behaviour Examples Certain security devices and elements (to be defined) must be monitored; a specific user or a designated role (to be defined) must be notified of any physical tampering with these devices or elements
Resistance to physical attack	Hierarchical to: no other components. FPT_PHP.3.1 The TSF shall resist [assignment: physical tampering scenarios] to the [assignment: list of TSF devices/elements] by responding automatically such that the TSP is not violated. Dependencies: No dependencies Examples The system must be resistant to physical tampering scenarios (to be defined) to system devices or elements (to be defined) by responding automatically such that the security policy is not violated
FPT_RCV: Trusted recovery	
Manual recovery	Hierarchical to: no other components. FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. Dependencies: FPT_TST.1 TSF testing AGD_ADM.1 Administrator guidance ADV_SPM.1 Informal TOE security policy model

	Examples After a failure or service discontinuity, the systems responsible for security must enter a maintenance mode where the ability to return the system to a secure state is provided
Automated recovery	Hierarchical to: FPT_RCV.1 FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.2.2 For [assignment: list of failures/service discontinuities], the TSF shall ensure the return of the TOE to a secure state using automated procedures. Dependencies: FPT_TST.1 TSF testing AGD_ADM.1 Administrator guidance ADV_SPM.1 Informal TOE security policy model Examples When automated recovery from a failure or service discontinuity is not possible, the systems responsible for security must enter a maintenance mode where the ability to return the system to a secure state is provided
Automated recovery	Hierarchical to: FPT_RCV.1 FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.2.2 For [assignment: list of failures/service discontinuities], the TSF shall ensure the return of the TOE to a secure state using automated procedures. Dependencies: FPT_TST.1 TSF testing AGD_ADM.1 Administrator guidance ADV_SPM.1 Informal TOE security policy model Examples For certain failures or service discontinuities (to be defined), returning the system to a secure state must be ensured using automated recovery procedures
Automated recovery without undue loss	Hierarchical to: FPT_RCV.2 FPT_RCV.3.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.3.2 For [assignment: list of failures/service discontinuities], the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.3.3 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of TSF data or objects within the TSC. FPT_RCV.3.4 The TSF shall provide the capability to determine the objects that were or were not capable of being recovered. Dependencies: FPT_TST.1 TSF testing AGD_ADM.1 Administrator guidance ADV_SPM.1 Informal TOE security policy model

	Examples For an automated recovery without undue loss, the functions provided to recover from failure or service discontinuity must ensure that the secure initial state is restored without exceeding a data loss limit (to be defined)
Automated recovery without undue loss	Hierarchical to: FPT_RCV.2 FPT_RCV.3.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.3.2 For [assignment: list of failures/service discontinuities], the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.3.3 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of TSF data or objects within the TSC. FPT_RCV.3.4 The TSF shall provide the capability to determine the objects that were or were not capable of being recovered. Dependencies: FPT_TST.1 TSF testing AGD_ADM.1 Administrator guidance ADV_SPM.1 Informal TOE security policy model Examples It must be possible to determine the objects that were or were not capable of being recovered
Function recovery	Hierarchical to: no other components. FPT_RCV.4.1 The TSF shall ensure that [assignment: list of SFs and failure scenarios] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state. Dependencies: ADV_SPM.1 Informal TOE security policy model Examples For identified failure scenarios (to be defined), security functions must either complete successfully, or recover to a consistent and secure state
FPT_RPL: Replay detection	
Replay detection	Hierarchical to: no other components. FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: [assignment: list of identified entities]. Dependencies: No dependencies Examples For certain identified entities (to be defined) replay must be detected
Replay detection	Hierarchical to: no other components. FPT_RPL.1.2 The TSF shall perform [assignment: list of specific actions] when replay is detected. Dependencies: No dependencies

	Examples Specific actions (to be defined) must be performed when replay is detected
FPT_RVM: Reference mediation	
Non-bypassability of the TSP	Hierarchical to: no other components. FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. Dependencies: No dependencies Examples Security policy enforcement functions must be invoked and succeed before each function within the system is allowed to proceed
FPT_SEP: Domain separation	
TSF domain separation	Hierarchical to: no other components. FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC. Dependencies: No dependencies Examples The systems responsible for security must maintain a security domain for their own execution that protect them from interference and tampering by untrusted subjects
TSF domain separation	Hierarchical to: no other components. FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC. Dependencies: No dependencies Examples A separation between the security domains of subjects must be enforced in the system
SFP domain separation	Hierarchical to: FPT_SEP.1 FPT_SEP.2.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.2.2 The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.2.3 The TSF shall maintain the part of the TSF related to [assignment: list of access control and/or information flow control SFPs] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs. Dependencies: No dependencies

	Examples The security systems responsible for access control or information flow control must be maintained in a security domain for their own execution that protects them from interference and tampering by untrusted subjects
SFP domain separation	Hierarchical to: FPT_SEP.1 FPT_SEP.2.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.2.2 The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.2.3 The TSF shall maintain the part of the TSF related to [assignment: list of access control and/or information flow control SFPs] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs. Dependencies: No dependencies ExamplesThe unisolated portion of a system responsible for security must maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects
Complete reference monitor	Hierarchical to: FPT_SEP.2 FPT_SEP.3.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.3.2 The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.3.3 The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFPs in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP. Dependencies: No dependencies Examples The parts of security systems responsible for access control or information flow control must be maintained in a security domain for their own execution that protects them from interference, tampering and untrusted subjects
FPT_SSP: State synchrony protocol	
Simple trusted acknowledgement	Hierarchical to: no other components. FPT_SSP.1.1 The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission. Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection Examples A system responsible for security must acknowledge the receipt of unmodified security system data when requested by another system responsible for security
Mutual trusted acknowledgement	Hierarchical to: FPT_SSP.1 FPT_SSP.2.1 The TSF shall acknowledge, when requested by another part of

	the TSF, the receipt of an unmodified TSF data transmission. FPT_SSP.2.2 The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements. Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection Examples For a mutual trusted acknowledgement, the concerned systems responsible for security must know the correct status of transmitted data among their different parts by the use of acknowledgements
FPT_STM: Time stamps	
Reliable time stamps	Hierarchical to: no other components. FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use. Dependencies: No dependencies Examples A system responsible for security must be able to provide reliable time stamps for its own use
FPT_TDC: Inter-TSF TSF data consistency	
Inter-TSF basic TSF data consistency	Hierarchical to: no other components. FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product. Dependencies: No dependencies Examples Certain types of security data (to be defined) must be able to be consistently interpreted when shared between a system responsible for security and another trusted IT product
Inter-TSF basic TSF data consistency	Hierarchical to: no other components. FPT_TDC.1.2 The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product. Dependencies: No dependencies Examples Interpretation rules (to be defined) must be used by systems responsible for security for interpreting security data from another trusted IT product
FPT_TRC: Internal TOE TSF data replication consistency	
Internal TSF consistency	Hierarchical to: no other components. FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE. Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection Examples

	Security data must be consistent when replicated between parts of the system
Internal TSF consistency	Hierarchical to: no other components. FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [assignment: list of SFs dependent on TSF data replication consistency]. Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection Examples When parts of the system containing replicated security data are disconnected, the consistency of the replicated data upon reconnection must be assured before processing any security requests using this data
FPT_TST: TSF self test	
TSF testing	Hierarchical to: no other components. FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF. Dependencies: FPT_AMT.1 Abstract machine testing Examples A system responsible for security must run a suite of self tests during initial start-up to demonstrate its correct operation
TSF testing	Hierarchical to: no other components. FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF. Dependencies: FPT_AMT.1 Abstract machine testing Examples A system responsible for security must run a suite of self tests periodically during normal operation to demonstrate its correct operation
TSF testing	Hierarchical to: no other components. FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF. Dependencies: FPT_AMT.1 Abstract machine testing Examples A system responsible for security must run a suite of self tests at the request of the authorized user to demonstrate its correct operation
TSF testing	Hierarchical to: no other components. FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at

	the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF. Dependencies: FPT_AMT.1 Abstract machine testing Examples A system responsible for security must run a suite of self tests in specific conditions (to be defined) to demonstrate its correct operation
TSF testing	Hierarchical to: no other components. FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data. Dependencies: FPT_AMT.1 Abstract machine testing Examples Authorized users must have the capability to verify the integrity of security data
TSF testing	Hierarchical to: no other components. FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. Dependencies: FPT_AMT.1 Abstract machine testing Examples Authorized users must have the capability to verify the integrity of executable code stored in a system responsible for security

3.1.9 FRU : Resource utilisation

FRU_FLT: Fault tolerance	
Degraded fault tolerance	Hierarchical to: no other components. FRU_FLT.1.1 The TSF shall ensure the operation of [assignment: list of TOE capabilities] when the following failures occur: [assignment: list of type of failures]. Dependencies: FPT_FLS.1 Failure with preservation of secure state Examples For degraded fault tolerance, certain system capabilities (to define) must be ensured when certain failures (to be defined) occur
Limited fault tolerance	Hierarchical to: FRU_FLT.1 FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [assignment: list of type of failures]. Dependencies: FPT_FLS.1 Failure with preservation of secure state Examples For limited fault tolerance, all system capabilities must be ensured when certain failures (to be defined) occur
FRU_PRS: Priority of service	
Limited priority of service	Hierarchical to: no other components.

	FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF. FRU_PRS.1.2 The TSF shall ensure that each access to [assignment: controlled resources] shall be mediated on the basis of the subjects assigned priority. Dependencies: No dependencies Examples For limited priority of service, each access to controlled resources (to be defined) must be mediated on the basis of the subjects assigned priority
Limited priority of service	Hierarchical to: no other components. FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF. FRU_PRS.1.2 The TSF shall ensure that each access to [assignment: controlled resources] shall be mediated on the basis of the subjects assigned priority. Dependencies: No dependencies Examples A priority must be assigned to each subject
FRU_RSA: Resource allocation	
Maximum quotas	Hierarchical to: no other components. FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment: controlled resources] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time]. Dependencies: No dependencies Examples Maximum quotas must be enforced for identified controlled resources (to be defined) that individual users, groups of users or subjects (to be defined) can use simultaneously or over a specified period of time
Minimum and maximum quotas	Hierarchical to: FRU_RSA.1 FRU_RSA.2.1 The TSF shall enforce maximum quotas of the following resources [assignment: controlled resources] that [selection: individual user, defined group of users] can use [selection: simultaneously, over a specified period of time]. FRU_RSA.2.2 The TSF shall ensure the provision of minimum quantity of each [assignment: controlled resource] that is available for [selection: an individual user, defined group of users, subjects] to use [selection: simultaneously, over a specified period of time] Dependencies: No dependencies Examples For minimum quotas, a minimum quantity of each identified controlled resource (to be defined) must be provided, for simultaneous use or over a specified time period, to a user, a group of users or subjects

3.1.10 FTA : TOE access

FTA_LSA: Limitation on scope of selectable attributes	
Limitation on scope of	Hierarchical to: no other components.

selectable attributes	FTA_LSA.1.1 The TSF shall restrict the scope of the session security attributes [assignment: session security attributes], based on [assignment: attributes]. Dependencies: No dependencies Examples The scope of session security attributes (to be defined) must be restricted based on certain attributes (to be defined)
FTA_MCS: Limitation on multiple concurrent sessions	
Basic limitation on multiple concurrent sessions	Hierarchical to: no other components. FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user. FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: default number] sessions per user. Dependencies: FIA_UID.1 Timing of identification Examples The maximum number of concurrent sessions that belong to the same user must be restricted
Basic limitation on multiple concurrent sessions	Hierarchical to: no other components. FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user. FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: default number] sessions per user. Dependencies: FIA_UID.1 Timing of identification Examples A limit on the number of sessions per user (to be defined) must be enforced by default
Per user attribute limitation on multiple concurrent sessions	Hierarchical to: FTA_MCS.1 FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [assignment: rules for the number of maximum concurrent sessions]. FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [assignment: default number] sessions per user. Dependencies: FIA_UID.1 Timing of identification Examples For a per user attribute limitation on multiple concurrent sessions, the maximum number of concurrent sessions that belong to the same user must be restricted according to rules (to be defined) based on user attributes
FTA_SSL: Session locking	
TSF-initiated session locking	Hierarchical to: no other components. FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: time interval of user inactivity] by: a) clearing or overwriting display devices, making the current contents

	unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session. FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: events to occur]. Dependencies: FIA_UAU.1 Timing of authentication Examples An interactive session must be locked after a time interval of user inactivity (to be defined) by making the contents of display devices unreadable and by disabling all means of accessing data other than unlocking the session
TSF-initiated session locking	Hierarchical to: no other components. FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: time interval of user inactivity] by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session. FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: events to occur]. Dependencies: FIA_UAU.1 Timing of authentication Examples Certain events (to be defined) must occur prior to unlocking the session
User-initiated locking	Hierarchical to: no other components. FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session, by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session. FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: events to occur]. Dependencies: FIA_UAU.1 Timing of authentication Examples The user must be able to lock the user's own interactive session by making the contents of display devices unreadable and by disabling all means of accessing data other than unlocking the session
TSF-initiated termination	Hierarchical to: no other components. FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: interval of user inactivity]. Dependencies: No dependencies Examples An interactive session must be terminated after an interval of user inactivity (to be defined)

FTA_TAB: TOE access banners	
Default TOE access banners	Hierarchical to: no other components. FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE. Dependencies: No dependencies Examples Before establishing a user session, an advisory warning message must be displayed regarding unauthorized use of the system
FTA_TAH: TOE access history	
TOE access history	Hierarchical to: no other components. FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [selection: date, time, method, location] of the last successful session establishment to the user. Dependencies: No dependencies Examples Upon successful session establishment, the date, time, method and location of the last successful session establishment must be displayed to the user
TOE access history	Hierarchical to: no other components. FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [selection: date, time, method, location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment. Dependencies: No dependencies Examples Upon successful session establishment, the date, time, method and location of the last unsuccessful session establishment and the number of unsuccessful attempts since the last successful establishment must be displayed
TOE access history	Hierarchical to: no other components. FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information. Dependencies: No dependencies Examples Access history information must not be erased from the user interface without giving the user an opportunity to review the information
FTA_TSE: TOE session establishment	
TOE session establishment	Hierarchical to: no other components. FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: attributes]. Dependencies: No dependencies Examples

	Session establishment must be able to be refused based on certain attributes (to be defined)

3.1.11 FTP : Trusted path/channels

FTP_ITC: Inter-TSF trusted channel	
Inter-TSF trusted channel	Hierarchical to: no other components. FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. Dependencies: No dependencies Examples A communication channel that is logically distinct from other channels and provides assured identification of its end points and protection of the channel data from modification or disclosure must be provided with each trusted IT product
Inter-TSF trusted channel	Hierarchical to: no other components. FTP_ITC.1.2 The TSF shall permit [selection: the TSF, the remote trusted IT product] to initiate communication via the trusted channel. Dependencies: No dependencies Examples Communication via a trusted channel must be able to be initiated by the system or by the concerned trusted IT product
Inter-TSF trusted channel	Hierarchical to: no other components. FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required]. Dependencies: No dependencies Examples The system must initiate communication via the trusted channel for functions for which a trusted channel is required
FTP_TRP: Trusted path	
Trusted path	Hierarchical to: no other components. FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. Dependencies: No dependencies Examples A communication path that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure must be provided between the system and a user
Trusted path	Hierarchical to: no other components.

	FTP_TRP.1.2 The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path. Dependencies: No dependencies Examples Communication via the trusted path must be able to be initiated by the system, the local users or by remote users
Trusted path	Hierarchical to: no other components. FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]]. Dependencies: No dependencies Examples The use of the trusted path must be required for initial user authentication and for other services (to be defined)

3.2 Requirements taken from ISO 17799

3.2.1 BPS : Security policy (Chapter 3)

BPS_PSI: Information security policy (§3.1)	
BPS_PSI.1.1	A security policy document must be produced and approved by management
BPS_PSI.1.2	The security policy must be communicated to all employees
BPS_PSI.1.3	The security policy must include a definition of general and specific responsibilities
BPS_PSI.1.4	The security policy must define clear and applicable security rules that cover all security aspects
BPS_PSI.1.5	The security policy must contain rules on the classification of information
BPS_PSI.2.1.1	The security policy must be regularly reviewed and in the case of changes that have an influence upon it, ensure that it continues to be appropriate
BPS_PSI.2.1.2	Security policy updates must be under the responsibility of a group or review committee whose members are identified
BPS_PSI.2.1.3	The security policy group or review committee must rely on the work of the security management group (see BOS_ISI.1.2)
BPS_PSI.2.2	Conformity of information systems with the security policy must be examined before opening any new IS services
BPS_PSI.2.3	A review procedure of policy or security policy rules must exist in function to information collected regarding declared security incidents (type, frequency, costs induced...)
BPS_PSI.2.4	The appropriateness of the security policy to business risk must be regularly verified (for example in the context of a global audit policy)

3.2.2 BOS : Organisational security (Chapter 4)

BOS_ISI: Information security infrastructure (§4.1)	
BOS_ISI.1.1	A security management group must be established so that there is clear direction and visible management support for security initiatives
BOS_ISI.1.2	The security management group must work recurrently upon the state of information system security (reported incidents, advancement of action plans, new services...)
BOS_ISI.2.1	If possible, the coordination and the implementation of security control measures must be the responsibility of a cross-sectional forum of management representatives from the relevant parts of the organisation
BOS_ISI.3.1	Responsibilities for the protection of individual assets and information as well as carrying out specific security processes must be clearly defined.
BOS_ISI.3.2	The security policy must provide general guidance on the allocation of security responsibilities.
BOS_ISI.3.3	General guidance for the security policy on the allocation of security responsibilities can be supplemented with more detailed guidance for specific sites, systems or services
BOS_ISI.4.1	A management authorization process for new information processing facilities must be established.
BOS_ISI.5.1	The organisation must establish a technology watch adapted to its environment and risks (vulnerability follow up and correction for example)
BOS_ISI.5.2	It must be possible to request advice from internal or external specialists (including national organisations specialising in information system security such as the DCSSI or the CNIL) regarding information security
BOS_ISI.5.3	Specialist advice must be communicated throughout the organisation

BOS_ISI.6.1	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators must be maintained
BOS_ISI.6.2	In the event of a security incident, the contacts mentioned in BOS_ISI.6.1 must be able to be used so as to ensure that appropriate action can be quickly taken (advice obtained, action taken by partners...
BOS_ISI.6.3	Exchanges with the contacts mentioned in BOS_ISI.6.1 must not endanger the protection of security information
BOS_ISI.7.1	The implementation of the information security policy must be independently reviewed (for example by an internal or external organisation that has no other operational responsibility in the domain of security)
BOS_SAT: Security of third party access (§4.2)	
BOS_SAT.1.1	An inventory of the nature of third party access to the information system (logical and physical access) must be made and a risk analysis must be carried out for each access listed
BOS_SAT.1.2	Appropriate measures of controlling secure access to the information system by third parties must be implemented
BOS_SAT.1.3	Each time a third party must access the information system, the person in charge in the organisation must have the means of controlling the operations performed
BOS_SAT.1.4	Access to the information system by third parties must be motivated by a functional need
BOS_SAT.1.5	Access to the information system by on-site third parties must not be implemented before appropriate control mechanisms are in place and a contract defining the terms of access is signed
BOS_SAT.2.1	Measures involving third party access to organisational information processing facilities must be based on a contract in due form containing all necessary security requirements
BOS_SOT: Outsourcing (§4.3)	
BOS_SOT.1.1	The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks and/or desk top environments should be addressed in a contract agreed between the parties.
BOS_SOT.1.2	Outsourced service contracts must define responsibilities between the parties and possible recourses in case of failure to respect the contract

3.2.3 BCM : Asset classification and control (Chapter 5)

BCM_RLC: Accountability for assets (§5.1)	
BCM_RLC.1.1	A global inventory of assets and services (including associated licences), permitting at least to identify sensitive and essential elements, must be drawn up
BCM_CLI: Information classification (§5.2)	
BCM_CLI.1.1	Classifications and associated protective controls for information must take into account company needs to share or restrict information and the business impacts associated with such needs
BCM_CLI.1.2	If possible, the responsibility for defining the classification of an item of information and for periodically reviewing that classification must remain with the originator or nominated owner of the information
BCM_CLI.2.1	A set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by the organization

3.2.4 BSP : Personnel security (Chapter 6)

BSP_SPR: Security in job definition and resourcing (§6.1)	
BSP_SPR.1.1	Security roles and responsibilities, as laid down in the organization's information security policy must be documented in the job description where appropriate.

BSP_SPR.2.1	Verification checks on permanent staff must be carried out at the time of job applications
BSP_SPR.3.1	Employees must sign a non-disclosure agreement as part of their initial conditions of employment.
BSP_SPR.4.1	The terms and conditions of employment should state the employee's responsibility for information security.
BSP_FOU: User training (§6.2)	
BSP_FOU.1.1	All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures.
BSP_FOU.2.1	All employees of the organization and, where relevant, third party users, should receive appropriate training in the use of tools (particularly putting new tools into production)
BSP_RIS: Responding to security incidents and malfunctions (§6.3)	
BSP_RIS.1.1	Security incidents should be reported through appropriate management channels as quickly as possible after their discovery.
BSP_RIS.2.1	Users of information services must note and report any observed or suspected security weaknesses in, or threats to, systems or services
BSP_RIS.3.1	Procedures for reporting software malfunctions must be established and followed
BSP_RIS.4.1	Mechanisms must be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.
BSP_RIS.5.1	There should be a formal disciplinary process for employees who have violated organizational security policies and procedures
BSP_RIS.5.2	The disciplinary measures for violating security policies and procedures must be communicated to all employees

3.2.5 BPE : Physical and environmental security (Chapter 7)

BPE_ZOS: Secure areas (§7.1)	
BPE_ZOS.1.1	Organisations must use security perimeters to protect zones containing information processing facilities
BPE_ZOS.2.1	Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
BPE_ZOS.3.1	Secure zones must be created so as to protect offices, rooms and facilities having special security requirements
BPE_ZOS.4.1	Additional controls and guidelines for working in the secure area must be used to increase the security provided by physical security measures that protect secure areas
BPE_ZOS.5.1	Delivery and loading areas must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
BPE_SEM: Equipment security (§7.2)	
BPE_SEM.1.1	Equipment must be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
BPE_SEM.2.1	Equipment should be protected from power failures and other electrical anomalies.
BPE_SEM.3.1	Power and telecommunications cabling carrying data or supporting information services must be protected from interception
BPE_SEM.3.2	Power and telecommunications cabling carrying data or supporting information services must be protected from damage
BPE_SEM.4.1	Equipment must be maintained in accordance with the supplier's recommended service intervals and specifications to ensure its continued availability and integrity
BPE_SEM.5.1	Security control measures and procedures must be used so as to protect

	equipment used outside an organization's premises
BPE_SEM.6.1	Information held on equipment must be erased before equipment is disposed of or reused
BPE_MMG: General controls (§7.3)	
BPE_MMG.1.1	Organizations must adopt a clear desk and a clear screen policy in order to reduce the risks of unauthorized access, loss of, and damage to information
BPE_MMG.2.1	No equipment, information or software must be taken off-site without authorization.

3.2.6 BGC : Communications and operations management (Chapter 8)

BGC_PRE: Operational procedures and responsibilities (§8.1)	
BGC_PRE.1.1	Operating procedures must be documented and maintained
BGC_PRE.2.1	Changes to information processing facilities and systems must be controlled by those in charge of the concerned facilities
BGC_PRE.2.2	Changes to information processing facilities and systems must be documented
BGC_PRE.3.1	Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to security incidents
BGC_PRE.4.1	Responsibility and areas of responsibility must be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services
BGC_PRE.5.1	Development, test and operational facilities must be kept separated
BGC_PRE.6.1	Before using external contractors to manage information processing facilities, the risks must be identified in advance, and appropriate controls agreed with the contractor and incorporated into the contract
BGC_PRS: System planning and acceptance (§8.2)	
BGC_PRS.1.1	Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance.
BGC_PRS.2.1	Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance.
BGC_PLM: Protection against malicious software (§8.3)	
BGC_PLM.1.1	Detection and prevention controls must be implemented to provide protection against malicious software, in addition to implementing appropriate procedures to promote user awareness
BGC_INT: Housekeeping (§8.4)	
BGC_INT.1.1	Back-up copies of essential business information and software must be taken regularly.
BGC_INT.2.1	Operational staff must maintain a log of their activities.
BGC_INT.3.1	Faults must be reported and corrective action taken.
BGC_GER: Network management (§8.5)	
BGC_GER.1.1	A range of controls must be implemented to achieve and maintain security in computer networks
BGC_MSS: Media handling and security (§8.6)	
BGC_MSS.1.1	Management of removable computer media, such as tapes, disks, cassettes and printed reports must be controlled
BGC_MSS.2.1	Computer media must be securely disposed of when no longer required
BGC_MSS.3.1	Procedures for the handling and storage of information must be established in order to protect such information from unauthorized disclosure or misuse
BGC_MSS.4.1	System documentation must be protected from unauthorized access
BGC_EIL: Exchanges of information and software (§8.7)	

BGC_EIL.1.1	Agreements, some of which may be formal, must be established for the exchange of information and software between organizations
BGC_EIL.2.1	During physical transport, media must be protected from all unauthorized access, misuse or modification
BGC_EIL.3.1	Electronic commerce must be protected from fraudulent activity, contract dispute and disclosure or modification of information
BGC_EIL.4.1	A policy must be drawn up regarding the use of electronic mail and control measures must be implemented to reduce security risks created by electronic mail.
BGC_EIL.5.1	Policies and guidelines must be prepared and implemented to control the business and security risks associated with electronic office systems.
BGC_EIL.6.1	There must be a formal authorization process before information is made publicly available and information integrity must be protected from any unauthorized modification
BGC_EIL.7.1	Procedures and controls must be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.

3.2.7 BMA : Access control (Chapter 9)

BMA_EMA: Business requirement for access control (§9.1)	
BMA_EMA.1.1	Business requirements for access control must be defined and documented and access must be restricted to what is defined in the access control policy
BMA_GAU: User access management (§9.2)	
BMA_GAU.1.1	There must be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services
BMA_GAU.2.1	The allocation and use of privileges must be restricted and controlled
BMA_GAU.3.1	The allocation of passwords must be controlled through a formal management process
BMA_GAU.4.1	A formal review process of users' access rights must be conducted at regular intervals
BMA_REU: User responsibilities (§9.3)	
BMA_REU.1.1	Users must follow good security practices in the selection and use of passwords
BMA_REU.2.1	Users must ensure that unattended equipment has appropriate protection
BMA_MAR: Network access control (§9.4)	
BMA_MAR.1.1	Users must only be provided with direct access to the services that they have been specifically authorized to use
BMA_MAR.2.1	The path from the user terminal to the computer service must be controlled.
BMA_MAR.3.1	Access by remote users must be subject to authentication
BMA_MAR.4.1	Connections to remote computer systems must be authenticated
BMA_MAR.5.1	Access to diagnostic ports must be securely controlled
BMA_MAR.6.1	Controls must be introduced within the network to segregate groups of information services, users and information systems
BMA_MAR.7.1	The connection capability of users must be restricted in shared networks, in conformity with the access control policy of BMA_EMA.1.1
BMA_MAR.8.1	Shared networks must have routing controls to ensure that computer connections and information flows do not breach BMA_EMA.1.1
BMA_MAR.9.1	A clear description of the security attributes of all services used by the organization must be provided
BMA_MAS: Operating system access control (§9.5)	
BMA_MAS.1.1	Automatic terminal identification must be used to authenticate connections to specific locations and to portable equipment

BMA_MAS.2.1	Access to information services must be attainable via a secure log-on process
BMA_MAS.3.1	All users must have a unique identifier (user ID) for their personal and sole use so that activities can subsequently be traced to the responsible individual
BMA_MAS.4.1	Password management systems must provide an effective, interactive facility, which ensures quality passwords (no passwords too short or too simple, no reuse or previous passwords...)
BMA_MAS.5.1	The use of system utility programs must be restricted and tightly controlled
BMA_MAS.6.1	A duress alarm must be provided for users who might be the target of coercion
BMA_MAS.7.1	Inactive terminals in high risk locations or serving high risk systems must shut down after a defined period of inactivity to prevent access by unauthorized persons
BMA_MAS.8.1	Restrictions on connection times must be used to provide additional security for high-risk applications
BMA_MAA: Application access control (§9.6)	
BMA_MAA.1.1	Access to information and application system functions must be restricted in conformity with the access control policy of BMA_EMA.1.1
BMA_MAA.2.1	Sensitive systems must have a dedicated (isolated) computing environment
BMA_SAS: Monitoring system access and use (§9.7)	
BMA_SAS.1.1	Audit logs recording exceptions and other security-relevant events must be produced and kept for an agreed period to assist in future investigations and access control monitoring
BMA_SAS.2.1	Procedures for monitoring use of information processing facilities must be established and monitoring results must be regularly examined
BMA_SAS.3.1	Computer clocks must be synchronized to ensure accurate audit logs
BMA_IMT: Mobile computing and teleworking (§9.8)	
BMA_IMT.1.1	A formal policy must be established and suitable control mechanisms adopted to protect against the risks of working with mobile computing facilities
BMA_IMT.2.1	Policies and procedures must be established to authorize and control teleworking activities

3.2.8 BDM : Systems development and maintenance (Chapter 10)

BDM_ESS: Security requirements of systems (§10.1)	
BDM_ESS.1.1	Statements of business requirements for new systems, or enhancements to existing systems must specify the requirements for controls.
BDM_SSA: Security in application systems (§10.2)	
BDM_SSA.1.1	Data input to application systems must be validated to ensure that it is correct and appropriate
BDM_SSA.2.1	Validation checks must be incorporated into systems to detect any data corruption
BDM_SSA.3.1	Message authentication must be used for applications where there is a security requirement to protect the integrity of the message content
BDM_SSA.4.1	Data output from an application system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances
BDM_COC: Cryptographic controls (§10.3)	
BDM_COC.1.1	A policy on the use of cryptographic controls to protect information must be developed and followed
BDM_COC.2.1	Encryption must be enforced to protect sensitive or critical information
BDM_COC.3.1	Digital signatures must be used to protect the authenticity and integrity of electronic documents
BDM_COC.4.1	Non-repudiation services must be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action

BDM_COC.5.1	A management system based on an appropriate set of standards, procedures and methods must be used to support the organization's use of the two types of cryptographic techniques
BDM_SFS: Security of system files (§10.4)	
BDM_SFS.1.1	Control must be provided for the implementation of software on operational systems
BDM_SFS.2.1	Test data must be protected and controlled
BDM_SFS.3.1	Strict control must be maintained over access to program source libraries
BDM_SED: Security in development and support processes (§10.5)	
BDM_SED.1.1	The implementation of changes must be strictly controlled by using formal change control procedures in order to minimize the corruption of information systems
BDM_SED.2.1	The application systems must be reviewed and tested when changes occur
BDM_SED.3.1	Modifications to software packages should be discouraged and essential modifications must be strictly controlled
BDM_SED.4.1	The purchase, use and modification of programs must be controlled and verified to protect against the possibility of covert channels and Trojan code
BDM_SED.5.1	Control measures must be enforced to ensure the security of outsourced software development

3.2.9 BCA : Business continuity management (Chapter 11)

BCA_AGC: Aspects of business continuity management (§11.1)	
BCA_AGC.1.1	There must be a managed process in place for developing and maintaining business continuity throughout the organization
BCA_AGC.2.1	A strategy plan based on an appropriate risk assessment must be developed to determine the overall approach to business continuity
BCA_AGC.3.1	Plans must be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes
BCA_AGC.4.1	A single framework of business continuity plans must be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance
BCA_AGC.5.1	Business continuity plans must be tested regularly and maintained by regular reviews to ensure that they are up to date and effective

3.2.10 BCO : Compliance (Chapter 12)

BCO_CEL: Compliance with legal requirements (§12.1)	
BCO_CEL.1.1	All relevant statutory, regulatory and contractual requirements must be explicitly defined and documented for each information system
BCO_CEL.2.1	Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products
BCO_CEL.3.1	Important records of an organization must be protected from loss, destruction and falsification
BCO_CEL.4.1	Control measures must be enforced to protect personal data in a manner compliant to the pertinent legislation
BCO_CEL.5.1	Management must authorize the use of information processing facilities and control measures must be enforced to prevent improper use the facilities
BCO_CEL.6.1	Controls must be established to ensure conformity with agreements, laws, national regulations or other instruments to control the access to or use of cryptographic controls
BCO_CEL.7.1	When an action against a person involves the law, either civil or criminal, the

	evidence presented must conform to the rules for evidence laid down in the relevant law or in the rules of the specific court
BCO_CEL.7.2	When an action against a person involves the law, either civil or criminal, the evidence presented must conform to all published standards or codes of practice for the production of admissible evidence.
BCO_RPS: Reviews of security policy and technical compliance (§12.2)	
BCO_RPS.1.1	Managers must ensure that all security procedures within their area of responsibility are carried out correctly
BCO_RPS.1.2	All areas within the organization must submit to regular reviews to ensure compliance with security policies and standards
BCO_RPS.2.1	Information systems must be regularly checked for compliance with security implementation standards
BCO_CAS: System audit considerations (§12.3)	
BCO_CAS.1.1	Audits on operational systems must be carefully planned and agreed to minimize the risk of disruptions to business processes
BCO_CAS.2.1	Access to system audit tools must be protected to prevent any possible misuse or compromise

3.3 Systems security policies (PSSIs)

3.3.1 PSI : Security policy

PSI-01: Evolution of the ISS policy	Over time an organisation can change (organisational structure, duties, scope, strategic themes, values). Its information system is also subject to frequent modifications, as well as the threats and vulnerabilities that apply. Therefore a re-examination of the ISS policy is to be anticipated: - for each major evolution of the IS context; - in the case of changes in threats; - in the case of the evolution of security needs; - following an audit; - following a security incident; - systematically at defined intervals; on demand of an authority (security manager, management...) in the framework of a procedure to define in the ISS policy.
PSI-02: Diffusion of the ISS policy	The ISS policy and all its operational versions must be fully documented and up to date copies must be easily accessible to all personnel in the organisation. The ISS policy must be known by the all internal parties as well as, if need be, all individuals accessing the information system of the organisation (contractors, service providers, trainees...) However, it can contain confidential information and organisation personnel may be concerned in varying degrees in function to their role. Therefore it is recommended, if need be, to develop and distribute summaries which include detailed extracts of pertinent information in function to readership. The goal of these summaries is to permit each individual to be informed of the risks and to know the security rules in function to his needs.
PSI-03: Control of the enforcement of the ISS policy	It is advisable to plan out the procedures and means of internal controls of the application of the ISS policy and to complete these by the procedures and means of external audits. Publishing rules without providing the means of controlling their application is not an acceptable situation, particularly regarding security.
PSI-04: Protection of information entrusted to the organisation	This principal enables assuring the exhaustiveness of regulatory references. Information provisionally held by the organisation and which, because of the information owner, carry a particular protection classification or indication, have to be strictly protected using the same measures as those applied by the original organisation. These measures could follow on from the application of legal texts (law no.78-17 from the 6th of January 1978 relative to computers, to files and to liberties...), of interdepartmental instructions like, for example, those that treat respect of the classification of information relating to defence secrets [IGI 900], of the protection of information relating to national heritage [II 486] or of the establishment of a defence market [II 2000]. In the case where these rules do not derive from common regulations, one should formalize the commitment of parties regarding the information exchanged.
PSI-05: Adoption of a needs scale	A needs scale based on different security criteria (availability, integrity, confidentiality...) will facilitate an objective classification of the organisation's essential elements (information and functions). The methodological process of the ISS policy guide proposes an approach to draw up a needs scale. It specifies that an acceptability rating and reference values must be determined for each security criteria. The reference values must be objective, distinctive to the organisation and bound to its strategic orientations. In addition, in the model plan proposed in the ISS policy guide, it is recommended to include this needs scale in the ISS policy.
PSI-06: Criteria of determining security needs	The methodological process of the ISS policy guide proposes an approach to determine security needs (in terms of availability, integrity and confidentiality...) for essential elements (information and functions) according to the needs scale adopted.

Two cases are presented for identified essential elements:
- direct use of the needs scale for those which possess no classification;
- correspondence with the needs scale for those who already possess a classification (for example information of a defence secrecy nature, information that is sensitive, vital...).

Other than the information related to defence secrecy and nominative information to which the legislative texts in force must be applied, security needs will be determined according to the control of the origin of information, their interest and their validity with regards to their life cycle in the operational process of production:
- the control of the origin of information (unknown or foreign, public domain, client, supplier...) takes on major proportions regarding security; specific criteria can be planned in function to their source in view of estimating if it is compromising to collect them, if they are valid and if their characteristics conform to system expectations;
- the assessment of the interest and the validity of collected information is done by the application of criteria clearly defined by the organisation's management and the criteria can be concerned with a particular domain (R&D, quality round-tables, technology watch...).
Remark concerning sensitive information:

Sensitive information is information whose disclosure or modification can harm state interests or harm organisational interests and for whom a financial loss could, for example, lead to bankruptcy. As a consequence one must principally ensure information confidentiality and, quite often, respond to an important need of information integrity. The information classified in this category is:
- on one hand, information related to defence secrecy information in the sense of article 5 of [IGI 900]; the organisation is required to respect the classification rules specified in the regulation; additionally the organisation is obliged to implement the means so as to be in conformity with the regulation;
- on the other hand, sensitive information that is not classified as a secret of defence in the sense of article 4 of [REC 901], that is to say, information related to the mission or to the business of the organisation (for example, technological know-how or professional secrecy), information relative to propositions of sale or furthermore to intelligence on the state of security (for example, the results of internal audits).
The classification retained aims first and foremost at giving the user an accurate representation of the sensitivity of the information he is handling, then to facilitate its control and, as a consequence, to improve the protection of sensitive information. For information that is not the responsibility of [IGI 900] the classification chosen must be approved by the organisation.

Remark concerning vital information:

Information said to be "vital" is information whose existence is necessary to the correct functioning of the organisation. One must principally ensure their availability and, quite often, respond to an important need of information integrity. The information that one can identify as vital is:
- on one hand, the information related to defence secrecy information in the sense of article 6 of [IGI 900],
- on the other hand, information not related to defence secrecy information in the sense of article 5 of [REC 901] but necessary for system operation, as well as information not covered by article 5 (for example, the nomenclature of items for a production unit).
The classification retained aims first and foremost at giving the user an accurate representation of the sensitivity of the information he is handling, then to facilitate its control and, as a consequence, to improve the protection of vital information. For information that is not the responsibility of [IGI 900] the classification chosen must be approved by the organisation. In particular, one can plan the specification of a lower limit of availability of vital information (processed or being processed) below which the information system is declared inoperable.

	Remark concerning strategic information: Strategic information is information the knowledge of which is necessary to reach the objectives that correspond to the strategic orientation of the organisation. The information can be protected by legislation, but can equally be covered by contracts, conventions or agreement protocols that are protected by the civil code. The classification retained aims first and foremost at giving the user an accurate representation of the sensitivity of the information he is handling, then to facilitate its control and, as a consequence, to improve the protection of strategic information; the classification retained can be based on criteria that is distinctive to the organisation like, for example, a particular sector (studies, innovations, markets...), the value level accorded and the length of validity. Remark concerning nominative information: Article 4 of the law "Computing and Liberties" defines the notion of personal data: "nominative information is data that permits, in any form whatsoever, directly or indirectly, the identification of the natural persons to whom it applies, whether processing is performed by a natural person or an artificial person". The classification retained aims at facilitating control and, as a consequence, to improve the protection of nominative information in conformity with the law; the classification retained can be based on criteria that is distinctive to the organisation like, for example, a particular domain (medical, recruitment...), the type of poll or enquiry, the processing or storage location. Remarks concerning costly information: Costly information is information that is part of the organisation's assets and for which collection, processing, storing or transmission necessitates an important delay or a high cost of acquisition. The legislative provisions mentioned for strategic information can be applied to this category. The classification retained aims first and foremost at giving the user an accurate representation of the sensitivity of the information he is handling, then to facilitate its control and, as a consequence, to improve the protection of costly information; the classification retained can be based on criteria that is distinctive to the organisation like, for example, a particular sector (studies, innovations...), the origin and the cost level.
PSI-07: "Declassification" of information	The classification of information is sometimes attributed for a period of time. Rules must define the minimum periods according to the nature of the information.
PSI-08: "Surclassification" of information	The degree of protection must be proportional to the classification of information and systems. Although the use of a higher classification appears to guarantee better protection, systematic surclassification may bring about a loss of confidence as to classification methods. To avoid this one should: - avoid surclassing information; - periodically review the attributed classification.
PSI-09: Identification and reach of the classification of information	The identification of the classification must be clear, known to all and immediately recognizable. For documents, it must be integrated in graphical charts; for floppy disks and other computer media, in the procedures for the management of these media; for files, in the procedures of the management of computer resources. The machines belonging to a network processing confidential information or storing information of this type equally must be identified. It is important that the personnel are aware of the possibility that the classification of their organisation may not be equivalent to a classification attributed the information coming from other organisations. Conversely the classification defined for the organisation may only make sense within the ISS policy perimeter.

PSI-10: Definition and control of authorisations	The organisation that is owner of the information must be in a position to assign the authorisations related to the use of the information and the organisation has to define the rules that manage authorisations and perform the corresponding controls. Without being necessarily the owner of the information at a given moment, the organisation can nonetheless be the trustee. In this case, the organisation does not possess the decision-making power regarding the information being processed but it must respect the management rules defined by the owner (clients, subcontractors...) in function to the affected classification.
PSI-11: Criteria of internal distribution of information	To avoid indiscretion and leaks information and generally the associated media can only be used in an environment that meets the security requirements defined by the organisation. The control of internal distribution aims to ensure that information is available exclusively to individuals having the need to know in the context of their work. A control also allows to verify the conformity of recopying information to permissions granted by law (copyright), by legislation (defence secrecy) and to specific constraints of the organisation. The need to know (for confidentiality) can be extended to need to modify (for integrity), to use (for availability)...
PSI-12: Criteria of external diffusion of information	The uncontrolled availability of information requiring protection can cause harm to the organisation (for example, loss of credibility or brand image, appropriation of know-how...). The implementation of criteria allows ensuring that the information transmitted to the exterior of the organisation, if it is of a confidential nature, imposes the prior authorisation of the receiver or a contractual clause binding the organisations concerned; in the case of nominative information, the communication must be in accordance with the law. Additionally, in the context of this principle, it can be foreseen that external diffusion of information be performed by authorized personnel and according to a procedure of prior authorisation.

3.3.2 ORG : Security organisation

ORG-01: General responsibilities for the security of the information system of the organisation	The nomination of an RSSI (ISS manager) (or his equivalent) is necessary to ensure the overall responsibility of the elaboration, implementation and functioning of the management of the ISS in the organisation. This ISS manager is in charge of making an ISS policy respected at all levels and domains within the organisation. This manager, attached to the management of the organisation must be able to make the security aspect prevail over all private interests and integrate security in all projects that use or affect the information system. The implementation of this function is a strong and necessary signal of the importance the organisation places on its ISS policy. In government, the operational department of the ISS covers these responsibilities.
ORG-02: The responsibilities for the elaboration and the implementation of an ISS policy	The ISS policy concerns all vital functions of an organisation; effectively an organisation generally could not bear a prolonged failure of its information system or systems. Therefore the ISS policy assumes strategic importance: a rule must define the responsibilities for its elaboration and its inevitable changes within a steering committee, for example. Additionally, in the implementation phase of the ISS policy, the rule establishes the responsibilities of the qualified authorities in the implementation and the control of security instructions for the installation and operation of the means that make up the information system. The rule strongly highlights the necessity of integrating security at the design and development phase of any new project concerning the information system. The ISS policy also indicates that the ISS is not limited to technical aspects and evolutions but that it encompasses every evolution or modification of the organisation, of professional engagements...
ORG-03: Reach of	The general principal of awareness of the OECD states: "The designation and

responsibilities	responsibility of owners, suppliers, users of information systems and other parties concerned by information system security must be explicitly stated." It is fundamental that all domains concerned by security (security of infrastructures, security in projects and application domains, security of locales, security documentation...) have a designated manager and that all security tasks have been assigned. The organisation of security in each of these areas must include strategic, management and operations levels. In particular, there must exist a clear and unique identification of the security responsibility related to networks or transversal systems such as the company office network or access methods to external networks.
ORG-04 : Responsabilités du niveau décisionnel	It's up to the authority level to take all actions of conception and implementation of security that is adapted to the needs and objectives of the organisation and to ensure that application of the ISS policy is respected. (1) For a ministerial organisation, this level corresponds to a high level defence official commissioned by the minister; he is responsible for the application of provisions relative to defence secrecy, to secrecy protection and to the ISS. He can be assisted in his mission by an FSSI (ISS government representative) whose principal duties are [IGI 900], article 19 and [REC 901], article 18): - to specify the procedures of applying interdepartmental instructions; - to draw up and control the application of instructions particular to his minister; - to organize the awareness of authorities; - to ensure the liaison with specialized interdepartmental and ministerial commissions. (2) For a public or private organisation, this level corresponds to a high level security manager appointed by the board of directors; he is assisted in his mission by a security committee. The board of directors, based upon recommendations from the high level security manager, establish the major orientations of the ISS, in agreement with organisational objectives and the different policies implemented (policy of personnel management, budgetary, production...). Additionally this committee can be the validation authority of the ISS policy. The high level security manager oversees the application of the ISS policy. He participates in board of director deliberations for which he is the adviser for all questions relative to security such as the definition of objectives, allocation of resources and of personnel. The security committee, presided by the high level security manager, assembles all the security managers from the different organisational functions. He oversees the coordination and the implementation of the ISS policy: In particular he verifies the coherence of security rules and referees the eventual conflicts with the other rules and practices in use in the organisation. (3) An information system security team, at the disposal of the high level defence official (or he high level security manager), can be formed if the needs of the organisation require it. It assembles computer and telecommunication specialists, as well as the managers of the non-technological aspects of the information system, all trained in security and whose principal tasks are: - the preparation and the coordination of security activities; - the periodic evaluation of vulnerabilities; - the research for technical solutions and the elaboration of procedures; - the implementation of awareness campaigns and training; - providing security expertise upon request of the board of directors. The security team can be composed of permanent staff but in function to need (such as large projects requiring a major evolution of the IS) specialists or experts in the concerned domains can be temporarily employed.
ORG-05: Responsibilities at management level	As soon as the size of an organisation can justify it, sub-units will be identified (sites, IS departments, divisions...) with an implementation of "local" managers, a clearly defined delegation of responsibility and an efficient organisation of coordination with the central structure. For ministerial organisations, this level reports to the qualified authorities who

	are responsible for the security of the information system for which they are in charge ([IGI 900], article 20 and [REC 901], article 19. For a private organisation, this level belongs to the local security correspondent, whose function is dedicated to the ISS and who reports to the team managed by the ISS manager. Their job description is to steer or direct the implementation of the ISS policy at their level (corporate, services, establishment...) and, more precisely: - to ensure the respect of contractual and regulatory measures; - to elaborate the internal instructions and directives; - to ensure that internal security controls are correctly performed; - to organize personnel awareness. These authorities can draw from the competence of the security team. To carry out the ISS management missions, it is sometimes necessary to form dedicated steering committees: - for the follow-up of the application of the ISS policy; - for crisis management, related to the ISS; - for technology watch activities, following on from the ISS needs of the organisation, and the evolution of the ISS policy.
ORG-06: Responsibilities at an operational level	At all levels, the hierarchical authorities are personally responsible for the application of the measures, defined by the qualified authority, destined to ensure the ISS ([IGI 900], article 20 and [REC 901], article 19). All personnel belonging to or working on the premises of the organisation is implicated in the ISS and holds responsibilities which must be clearly formalized and communicated to all. Notably the responsibilities and obligations of personnel (see security principals related to contractual obligations) cover: - the respect of laws and regulations, - the respect of the specific policies and rules (related to a project, to an establishment, to a particular function), - the access to a network or to the premises of a different organisation. These responsibilities can be reinforced in relation to their functions and authorisations (see security principals related to authorisations). For example, information system administrators, as holders of secrets and who operate sensitive functions of information systems, will have particular responsibilities in the area of the ISS. In addition, the responsibilities of personnel in the organisation must also cover the case where they intervene in an IS other than the one of the organisation to which they belong (clients, partners...).
ORG-07: Other managers in the organisation that play a role in the ISS	There exist other non security-dedicated functions which nevertheless play a specific essential role in the operation of the ISS. Notably these functions are: - security officers or correspondents To permit the implementation of instructions and procedures at each site, department or unit, the hierarchical authorities are assisted by one or more security agents whose duties are principally to provide an interface between IS users and the managers in charge of the follow-up of the ISS. The objective is two-fold: o to facilitate the distribution of security information and the application of the rules of correct usage; o to assure user feedback to the centralized security follow-up. This role must be assured by individuals "close" to users, both in a geographical context and in the sense of professional orientation. These officers are the privileged correspondents of the security team. They could also be in charge of resources common to several operational units. Their role is therefore the implementation of measures of protection compatible to unit objectives and the local resolution of security problems. In the absence of such measures, a difficult arbitration between a functional task and a security action could ensue. - the managers of the legal department of the organisation

	They play an indispensable role in the ISS area of the organisation. Upon the initiative of the ISS manager, they intervene in diverse areas of which notably: o the drawing up of confidentiality clauses and engagements of the ISS in commercial contracts and employment contracts; o the filing of complaints and legal case work; o integration of the rules of the ISS in the different regulations and charters of the organisation; o relations with subcontractors. o the responsibilities of auditors Other than the responsibilities of control that are assigned to operational roles, the auditors have the responsibility of the following missions: o to define the audit strategy, including notably the ISS audits; o to perform or have performed the ISS audits, according to the audit plan or on request of directors, in relation to the ISS manager; o to inform the demander and the audited entities, according to their need to know, and to inform the ISS manager of the discovery of any eventual ISS incidents or anomalies. o other responsibilities can be necessary to accomplish specific security actions that are defined, for example, in the context of plans of security improvement, of application migration.
ORG-08: Specific entities dedicated to security management	Other specific entities can be created. Among these entities, one can name: - a security committee, responsible for the maintenance of the ISS policy and follow-up of the application of the priority action plan. The committee also has to keep executive management informed of the efficiency of the policy in place; - a crisis centre, responsible where relevant for implementing an emergency procedure to manage the situation; - a technology watch team, responsible for following up security alerts and their handling according to their criticality; - an audit centre, responsible for performing audits of the IS.
ORG-09: Application of the notion of responsibility-owner	The notion of responsibility-owner concerns the top manager of an entire entity (establishment, service, responsibility or profit centre) or the qualified authority as is defined in the principal ORG-05, Responsibilities at management level, and who disposes of his own human and material resources to achieve his mission. The term owner applies to information assets, to software and to the material constituents of the information system and implies the obligation to respect the laws, regulations and rules in application in the organisation. The information, software and materials concerned can belong to the organisation or have been given by a third party (clients, partners, service providers...). The responsibility-owner decides on the acceptable risk level and the conditions for accessing files, on up-dates of information (in conformity with the rules of classification in application in the organisation) or on modifications to software and to the materials of which he disposes.
ORG-10: Application of the notion of responsibility-holder	The responsibility-holder is authorized by the responsibility-owner to apply laws, regulations and the rules of protection concerning information, software and materials during the activities of their collection, processing, diffusion and storage. The responsibility-holder can be, for example, an information professional from the operational team, an information officer, a secretary... He is the guardian of a part of the information assets of the organisation and he is thus held, above all, to act as guarantor of the application of the law concerning the legal protection of the software entrusted him (illegal copies).
ORG-11: Management of relations with third parties intervening in the context of the ISS	The ISS policy must formalize the types of relations, the instructions and identify the useful contacts with third party organisations that play a role (or are likely to play a role) in the context of follow-up and maintenance of the ISS. Among these organisations, there can be: - in the category of authorities and partners: o the organisations to contact in the case of detection of a malicious act in the context of the IS; o the organisations of surveillance and alert;

	o the organisations of audit; - in the category of service providers: o service providers of telecommunications; o service providers working on the premises of the organisation; o service provider subcontractors and/or taking in charge a part of IS operations; o security expert service providers; o external organisations of audit. It is essential to control access, be it to the information system or even to sensitive information concerning the IS and its security. As soon as a third party, because of a service need, must have this type of access, it must be assured that the same security rules that apply to internal personnel are applicable (documentation and contractual aspects) and applied by the individuals concerned.
ORG-12: Contractual framework for the exchange of secure data	The propositions of access to services or to telematic applications that are internal or external to the organisation pose the problem of cooperation between the different information systems. This rule aims to prevent the loss, modification and misuse of data .As a consequence, one must plan the contractual responsibilities and obligations of the different parties, both from the point of view of data transfer as well as regarding the applications that perform this act. The exchange of secure data is situated in the context of data transfers as is defined above. The contractual context designates the agreements between several parties to exchange data by the use of information technology or not: this rule includes the case of the exchanges of computerized data (EDI). The agreements passed or contracts signed by the organisation with all information system users contain precise clauses of control, for example: - the responsibility of the management of exchange flows; - the procedures of security used for exchanges; - the standards of data structure; - the responsibilities in case of data loss; - the specific measures for the protection of cryptographic keys.
ORG-13 : Procedures of use of telecommunication networks external to the organisation	The use of telecommunication networks external to the organisation connects users who do not, a priori, have the same security requirements, and who, in addition, are not controllable. The practical details of secure use of telecommunication networks external to the organisation concern above all the control of means which can escape the centralized management of the information system like, for example, the installations of modems or Minitels. The special case of electronic mail has to prompt the adoption of measures aimed at controlling the sending of messages, considered vulnerable to non-authorized interception and modification, and of the legal implications related to the non-repudiation of the sent or received message. Organisation personnel who work from home (teleworking) are in a private environment over which the organisation has no control, this is why it must implement specific technical rules concerning access rights but also specifically make the user aware by informing him of his responsibilities regarding the company information he is entrusted with. The sections drawn from the OSI architecture apply to the case of networks external to the organisation.
ORG-14: Specific clauses of information protection	When exchanges are planned with third parties, specific clauses can be included in contracts, regulating the context of these exchanges. They affect the means, like: - the control of the absence of malicious code; - the protection rules applied internally (specification of a cross -classification table) - the exchange media and the means of protection against disclosure, integrity and non-repudiation... If the organisation commits to respect such clauses as set out by a third party, it must inform the personnel concerned, or include them in its ISS policy.

ORG-15: Selection, coordination and use of cryptographic means	Because of what is at stake, the selection of the means (for example software or usable cryptographic materials) and even more so of the external services (for example: certificate authority, service provider of confidence) must be validated and approved by the organisation's security structure when the selection is not directly made by this structure. One of the essential elements to take into account as far as confidentiality is concerned is managing the need (or lack of it) of the organisation recovering the documents that personnel have encrypted. The solutions can be done at the key management level (for example, implementation of sequestration) or at the level of functions and utilities (systematic creation of recovery fields). For each of these basic functions (confidentiality, authentication, non-repudiation) one should elaborate rules indicating the minimum requirements (basic and operational) that should be respected. The choice of external contractors (Certificate Authority (CA) or Certificate Service Provider (CSP) for example) is a structural decision that requires the approval of the security structure and a validation by executive management. One should ensure that acceptable clauses related to protection, security and guarantee are explicitly written in to each service provider contract.
ORG-16: Implementation of an organisation of surveillance and prevention	It is essential to define an organisation that surveys and maintains the list of major risks that hang over the information system (new threats, new security needs, major evolutions of the information system...). This organisation must dispose of the competence of internal or external experts and sufficient means to collect and qualify the information (contacts, subscriptions to specialized organisations, see ORG-11, Management of relations with third parties intervening in the context of the ISS. It must also dispose of controlled means of the diffusion of pertinent security information as a preventative measure. This vigil can be externalized or performed in liaison with organisations like CERTA who regularly publish advice, alerts or recommendations to the French administration. However, the implementation of a surveillance system must be accompanied by a follow-up of recommendations: surveillance is not a means to itself, it is imperative to control the implementation of the recommendations that result from surveillance.
ORG-17: Organisation of crisis centres	The principal is to firstly define an organisation (responsibilities, operational principals and means) that is able to respond to major incidents occurring to the information system. To do this one should plan escalation procedures, test them and train personnel in their execution. The major point is to identify the individuals at the correct management level so as to be able to take decisions as quickly as the situation merits. As well one should define the means and procedures able to: - spread the alert; - collect the information; - set up an emergency crew; - decide on conservation methods; draw up an action plan that draws together corrective measures.

3.3.3 GER : ISS risk management

GER-01: Definition of the management context of ISS risks	The management of ISS risks is a continuous process for which one should precisely define the context (resources, means responsibilities...) for each of these aspects: - risk assessment: this task consists of analysing and evaluating the ISS risk by comparing the risk level to previous defined risk criteria; - treatment of risk: this task consists of reducing, transferring or accepting the risk determined by the previous task; - accepting risk: this task consists of accepting the risk, and if need be to accept the residual risk; - communication related to risk: this task consists of exchanging or sharing information concerning risk.
GER-02 :	The identification of security objectives allows defining the real needs of the

Identification des objectifs de sécurité	organisation in terms of the ISS. This ISS specification can be drawn up by respecting the following steps, taking into account the mission or business of the organisation: - collection of strategic elements (constraints, stakes, strategic approaches, frame of reference...), - express the security needs of the essential elements (information and functions) in terms of availability, integrity, confidentiality... and according to an objective needs scale, - study of threats hanging over the organisation (character of threatening elements, vulnerability study...), - identification of real risks for the organisation. The security objectives must cover all the risks identified. Defining security needs allows describing in an unambiguous manner the sensitivity levels (in terms of confidentiality, integrity, and availability...) that one should ensure the elements of an information system. The security one expects from an information system must be defined in these specifications because it is an essential dimension of this system as well as the performance or services it must render: this expression of security needs should be thoroughly examined using a methodological approach and from an overall viewpoint. Using a methodology to perform this analysis allows retaining a consistent overall vision of the ISS problematic, creating a complete security frame of reference and becoming aware of the greatest number of risks the system carries. A risk assessment should also permit, at this stage, to expose the vulnerabilities of the system and the consequences of eventual security accidents in a manner so as to be able to justify the implementation of certain countermeasures whose cost efficiency will have been evaluated. Thus, for example, the results of a risk assessment could lead to taking out insurance to compensate for a lack of skills or budgetary resources. On the base of this analysis the decision can be taken to accept the risks or not.
GER-03 : Circumstances that justify a revaluation of the ISS	The principal of revaluation of the guidelines of the OECD that regulates the security of information systems and networks stipulates: "The representatives must examine and re-evaluate the security of information systems and introduce appropriate modifications in their policies, practices, measures and procedures of security. New vulnerabilities and new or evolving threats are constantly being discovered. All representatives must continuously review, re-evaluate and modify all aspects of security to combat these evolving threats." Once a system has been subjected to an evaluation, it is unrealistic to suppose that it is safe from errors or that modification is impossible: indeed, the system should meet new requirements which will lead to the modification of material, software and documentation. In addition, new security needs can appear and cause new risks that should be understood and acted upon. With this in mind, it is evident that certain modifications require a re-evaluation like, for example, the redevelopment of the operating system kernel, which can depend, in part, upon the results of the preceding evaluation. On the other hand, other modifications could lead to no new evaluation if they only concern parts of the information system that are separate from security components and do not influence it. In general, any evolution of the information system (human, organisational, financial, geographical...) should lead to reflection on the security plan. This reflection could lead to a re-evaluation of the system or simply a modification of certain rules.
GER-04: Prospective study on the evolution of the ISS	A prospective study on the evolution of the ISS allows anticipating the organisation's medium term needs and to integrate into its security, as soon as possible, the new objectives, software, materials or necessary mechanisms. This prospective study cannot be dissociated from strategic orientations (or from an IS master plan) concerning new information technologies susceptible to being chosen by the organisation.

	Additionally, this rule aims to verify that any evolution of the IS conforms to security principals in force in the organisation. If this is not the case, the prospective study allows measuring the impact this has on security and proposing technical or organisational changes that can lead to a modification of principals and rules of the ISS policy of the organisation.
GER-05 : Control of certain specific flows	When communication is allowed to be exchanged between the interior and the exterior of the IS of the organisation, as well as within the interior of the IS, or even for communication between enclosed perimeters it could become necessary to implement specific rules and means of control of these flows. Conducting a risk analysis using a methodology is of particular interest here because it permits clearly identifying all flows exchanged by the IS as well as threats to the flows.* It will be the case, for example, for email exchanges to the exterior with rules and thus the means to implement them concerning the size of exchanged messages, the nature of attached files (accepting or refusing active content), the anti-virus control and the control against malicious code. These different measures must be consistent with the security charter and with the proper use of computer resources that all users must have signed, because beyond his information regulatory aspects (obligation to inform personnel, privacy) come into play. Another example is outbound HTTP flows (consultation of external web servers from the workplace in the IS) with measures like, for example, the implementation, by the use of an outbound proxy, of authentication for outbound traffic, the storing of connection logs... It is beyond the scope here to identify all possible cases, even less to give for each the appropriate rules and means, the rule to remember is that each of these flows must be identified and analyzed from a security point of view and can/should lead to the implementation of specific solutions to ensure security.
GER-06: Identification of services and means that justify the use of cryptography	Given the technical and legal implications, it is important to identify the applications and services that require the use of cryptographic techniques. Cryptographic solutions must also be identified for each application or service. This choice is performed in function to the type of information processed and the regulatory context. For example, in the context of an IS that handles defence secrecy information, the use of certified cryptographic methods is compulsory. Here again the risk assessment provides the regulatory constraints concerned as well as the needs of users.

3.3.4 CDV : Security and life cycle

CDV-01: Integration of the ISS in projects	The ISS policy must make provision for an organisation that ensures taking security aspects into account during the entire life cycle of projects (kick-off study, feasibility study, detailed general conception...right up to obsolescence). This entity, although autonomous in relation to projects, must be closely integrated to the managers responsible for the direction and coordination of overall ISS in the organisation. In particular, the organisation must identify the domains and projects in which recognized experts must intervene.
CDV-02: Conditions of making any new IS element operational	This rules aims to reduce security risks due to a lack of cooperation with other elements of the environment or the inadequacy of the technical and human instructions in place which could be the source of operational errors. A new element of the information system (software or material), even if said to be efficient and in conformity with the manufacturer's specifications, must submit to integration tests its new environment. The conditions recommended by this rule can require, for example, comprehensive acceptance tests of the element so as to identify technical modifications and procedures to perform as well as the possibility, in case of failure, to perform a rollback of the technical environment to the previous state before the element was put into operation.
CDV-03: Control of software before it becomes operational	The controls of software before they become operational principally aims to combat the threat of contamination by viruses or other malicious code and the risk of the non-conformity of software. Viruses or other malicious code pose an increasingly serious problem for the ISS. Their existence affects all organisations and institutions no matter what their level

	of vulnerability. The organisations that are the most open to the public are the most exposed to computer pirates whose motivations are quite often those of performing technical feats and the media exposure. The risk of non conformance of software concerns the organisations that process sensitive data who, in the context of calling upon service providers for their software development, must verify the correctness and conformity of the program code so as to verify that the program only does what it was conceived to do and that no backdoors exist which would later permit an illegal modification of the program's functions. Precautions can be taken to prevent and detect introduction of fraudulent programs (viruses, worms, Trojan horses, logic bombs...). All digital storage media external to the organisation and, in particular, media of uncertain origin, are controlled. Implementing dedicated means of systematic monitoring constitutes a counter-measure to this threat.
CDV-04: Conditions for the implementation of security controls	The security manager controls the consistency and the validity of the programs of the acquisition of equipment in his organisation in relation the major orientations of security and the strategic orientations of the organisation. Additionally, and in the context of investigations begun at his request, controls are implemented by the security team. These controls are distinguished by their reach and their size: - their reach refers to defining their level of detail (this is the vertical component); - their size refers to the different elements taken into consideration by the control (this is the horizontal component). It is essential, to the climate of confidence for personnel and the smooth running of the organisation's mission, to adopt a graded approach in security controls, as a function of the circumstances as clearly stated by the decision making level; other than the legal or disciplinary context, these controls must be accompanied by communication and the preparation of personnel.
CDV-05: Security control procedures by the management level	The periodic re-evaluation of the vulnerabilities of entities (material, software, network, locales, organisations, personnel) in the face of threatening elements (accidental or deliberate, and natural, human or environmental) and their attack methods is necessary so as to assess the level of security of the information system. The qualified authorities, helped by the organisation's security team, establish the technical procedures, the methods and the tools necessary for security; they control their proper use and efficiency according to criteria set by the decision making level. These controls are part of the context of planned security inspections or audits that cover the different information system security entities (material, software, networks, locales, organisations, personnel). For the controls that require the use of operational and technical resources, the management level has to establish a plan whereby this does not become a hindrance to the smooth running of the organisation's mission.
CDV-06: Continuity of security control by the operational level	Security officers perform the controls allotted them by the application of tolerance levels fixed by the qualified authority. The observation of repeated deviations, related for example to operational constraints, or a change in the state of the information system, could lead the management level to modify these tolerances. Their actions of control are tightly linked to the execution of operational tasks and they concern ([IGI 900], article 20, [REC 901], article 190: - the protection of individuals like, for example, the update of the list of permanent employees and, if need be, affected to information processing, - the protection of information like, for example, the destruction of classified information that must be purged from the system, - the protection of systems and networks like, for example, the control of the distribution of authentication elements for classified applications to users. These controls are complimentary to those entrusted to engineers who treat audit logs.
CDV-07: Permanent control of the	The control of the integrity and the availability of the means of protection is a fundamental aspect of security. This rule concerns the security measures relied upon to ensure the protection of the processed information: it concerns

means of protection	equipment, mechanisms (material and software) and the associated documentation, cited in article 10 of [IGI 900], "Information Systems Security Controlled Articles" (ACSSI) or of article 9 of [REC 901]. The maintenance of this confidence justifies a control of the integrity and the availability of these means which have a life cycle: They are conceived, built, used, repaired, then declared unfit or destroyed. Their integrity and their availability, fundamental conditions for the efficiency of security, are guaranteed by the implementation of specific management measures including the most proactive maintenance program possible.
CDV-08: Application of code control and acceptance procedure	Development control procedures can be carried out to fight against the introduction of malicious functions (for example: peer review of code, sealing code under the responsibility of the developer, control by sampling...). All development or modification of code must be followed by procedures of unitary acceptance testing, integration and validation before its implementation. Particular attention must be paid to the control of values and limits.
CDV-09: Other types of necessary controls	Here are some other examples of controls to implement: - control of the application in projects of the standards set out in the ISS policy; - control of the coverage of the ISS policy in relation to the evolution of IS risks; - control of the correct application of access management rules and authorisations; - control of the respect of security rules by third parties (service outsourcing, facilities management); - control of the incident database and the completeness of actions; - control of the respect of the rules for physical access; - control of the regular analysis of activity logs notably those of accounts disposing of extended system privileges or that access sensitive/vital information or functions; - control of the presence of contractual security clauses in all service provider contracts; - control of the efficiency of the protective measures of the public network; - control of the application of acceptance procedures of a new information system or a major evolution before its implementation; - control of the respect of laws, regulations and the different codes of practice; -...
CDV-10: The control process must not impact on the operation of the IS	The control procedures must be clearly defined. The accesses and privileges necessary for testing and for controlling the information system must be controlled in time and in their reach. Particular attention must be paid to verify that performing these procedures does not have a significant impact on the operation of the information system.
CDV-11: Performance of a security audit	The efficiency of all means of security can only last if these means are regularly verified by the use of tangible elements. Security audits of the information system are performed by qualified and authorized individuals in accordance to defined procedures and in accordance to precise and validated procedures that permit the assurance of the correct application of security procedures, of the operational functioning of these procedures, of the consistency of these procedures, of the means in place and the effective implementation by these means of the entire target process, including evolutions. The results of these audits are distributed to the person behind the order and to individuals who need to know them. The discovery of incidents or failures of information system security must be reported to the ISS manager. External information system audits must be agreed in advance by the ISS manager. This type of audit must be performed within a strict framework in which the responsibilities of all parties are defined (depth of the investigation, distribution of results). As a complement to these audits, intrusive tests can be performed. These tests must be defined and supervised (choice of a contractor, confidentiality commitments, back-up procedures and start-up plan...).

3.3.5 ACR : Assurance and certification

ACR-01: Minimum	These requirements must be clearly stated and principally concern:

requirements of application software used in the IS	- the protection of configuration data and parameter settings: they are too often forgotten even though they represent one of the easiest and often one of the most difficult to detect means of misappropriation of application software; - the validation and the eventual filtering of input data before any processing: this validation must be planned and systematically applied but particularly concerns user "input" (risks of error or of malicious attempts) and external data; - the validation of output data: this is the equivalent of the previous and it concerns: - the protection of the processing inputs that follow in an application software chain, - and/or the reliability of the results at the end of the process; - the risk of data modification or corruption by the application software itself: these problems most often come from errors of conception and more so from set-up errors (bugs) which can be exploited by these malicious users; - the presence and the relevancy of mechanisms of automatic control from within the application software itself and their capacity to generate alert notices during abnormal or simply unexpected behaviour; - the presence and the relevancy of log and journal mechanisms that are available and configurable according to needs.
ACR-02: Definition of a security target	The security target constitutes the specification of the system in terms of security; it is a very important step which establishes at the same time the objective to reach and the means to obtain it. In the first place, the detailed thought process that resulted from the study of security needs and the risk analysis should permit a decision on what one finally decides to protect, by specifying the why, against whom and against what; the summary of this thought process constitutes the security objectives of the system. These security objectives are clearly defined from the specification phase so that one can reach them and then after evaluate if the security of the system is able to satisfy them. From these security objectives one decides on the measures to implement, either technical or non-technical. The non-technical measures are the procedures and the rules of implementation, of management and organisation, the authorisation of personnel, the measures contributing to the protection of the system environment and all the measures of a regulatory nature. The technical measures are the security functions that must be planned in the conception of the system so as to satisfy the objectives; these functions are performed through the means of security mechanisms integrated in the system. Objectives and functions constitute the key of the security target, it represents the security fundamental in the conception of the information system. However, so that one can be certain that the objectives are satisfied, on one side these functions and mechanisms must exist and, on the other, one must be able to have sufficient confidence in them.
ACR-03: Respect of security requirements before operational launch	The verification of the respect of requirements must be: - on one side, implemented by the selection (software purchased) or the specification (software developed) so that the intrinsic qualities of the software is sufficient to permit a launch from a security point of view; - on the other, performed in pre-operational conditions so that the security level is guaranteed in a real operational situation (environment, parameter setting...).
ACR-04 : Periodic verification of the respect of security requirements of application software	To provide protection against deviation over time, it is important to implement procedures of regular periodic control of the respect of security requirements on the characteristics and functioning of application software. Part of the control can be internal.
ACR-05: Evaluation of the confidence level granted the IS: evaluation and	The conception of the system is guided by a consistent approach which leads to the security objectives being reached; security functions are chosen to satisfy these objectives. Once the system is developed and in service, it must be known what continued

certification	confidence one can have that the security target is really reached. On one side this confidence depends on the choice of functions, of their efficiency and the quality of their development and, on the other, confidence depends on the manner in which the system was installed, made operational and used. The study of each of these aspects will allow justifiably having confidence in reaching the security target; it is the objective of the evaluation. A system that is developed according to the principals exposed above can be evaluated and one will thus have the confirmation that one can have confidence in it both as to the security it ensures regarding the information entrusted to it and as to the processes that use this information. The evaluation makes a significant contribution to the reduction of the risks of non-desired behaviour from an application. It consists of evaluating the properties of a system or of a product with regards to standardized security criteria, for example the Common Criteria. This evaluation must be made according to an approved method that respects defined rules. The results of the evaluation and the fact that the evaluation criteria used have been correctly applied are confirmed by a formal declaration called a certificate. However, certification is not obligatory: The demander of the evaluation is responsible for judging the need for certification.
ACR-06: Criteria of acquisition and conditions of use of software packages	If the criteria of purchasing software packages are essentially economic and operational (immediate availability of product, affordable price, maintenance and technical assistance), even so there still remains a problem of security regarding the integrity of the software delivered and its use within the organisation. It is therefore essential that a rule establishes the criteria that would permit the justification of buying software packages and their conditions of use which bear upon, for example, the following aspects: - verification of the respect of security principals in force in the organisation before the purchase decision is made; - conformity and integrity tests before the operational launch of software packages; - restrictions on use in function to the sensitivity of the work station.
ACR-07: Adoption of development methods and tools	The adoption, from the start of the conception of the information system, of development methods and tools is a sign of the organisation's desire to control security. The application of this rule allows justifiably acquiring confidence in the conception and in reaching the security target; it contributes to the implementation of united and consistent protection which forms a guarantee of success for a future evaluation of the information system. However, this rule does not suggest the use of a single method for the development of an information system but it calls for a surveillance of the needed consistency that must exist among the different methods used by the organisation.
ACR-08: Adoption of a programming and data coding standard	The adoption of a programming standard interests all computer application development, including the software parts that can contain material or different devices of the information system. The first recommendation related to the adoption of a programming standard is to specify the material and software configurations used for development. The second obligation concerns the choice of a model and a structure of programs that allows for uniform references recognized by all, thus facilitating software maintenance operations and the updating of technical documentation. Data coding concerns the format and the representation of data fields which, for the same reasons as for program structure, requires adopting a standard. The different states of output data also comply with presentation standards that take into account the functional particularities of users in the organisation. The data administrator is responsible for the correct definition of data and for the file and database structure.
ACR-09: Certification of the information	The security certification is the declaration by the certification authority (governmental or specific to the organisation in some cases), in view of the certification dossier, that the IS under consideration is apt to process information

system	at a given sensitivity or classification level in conformity to the aimed-for security objectives, and that the inferred residual security risks are accepted and controlled. To complete a certification successfully, a steering committee is generally in charge of managing the project. It manages the preparation of the entire certification dossier that the certification authority must approve. The security certification remains valid as long as the IS operates in the same conditions as was approved by the certification authority. It defines the acceptance of a level of residual risk that is qualified and quantified in terms of confidentiality, integrity, availability, authenticity and non-repudiation.
ACR-10 : Accreditation of the information system	The evaluation and the certification which confirms its results only allow to ensure that the security target is correctly reached. It only makes up one of the elements to judge if the system, or the product, as well as the non-technical security measures (in particular, the operational procedures effectively implemented), once in its real environment, properly presents the adapted protections to the sensitivity of the resources that it is in charge of and to the range of threats it must guard against. Moreover it is necessary to make a judgement on the relevancy of the security target in relation to the real environment of the system in operation: this is the role of accreditation for it represents the formal recognition that the product or the evaluated system can protect information up to a specified level, within the defined conditions of use.
ACR-11 : Management of security documentation	The management of security documentation includes accounting, up-dates, reproduction and destruction: - the management of security documentation relies on precise and efficient accounting based on an up-to-date inventory log, - regular up-dates of the security documentation is made compulsory by the constant evolution of the information system, - the reproduction and the destruction of documentation is done upon the security manager's orders who verifies that the operation is performed on the totality of the designated documents and those only.
ACR-12: Adoption of a standard for elaborating security documentation	The diversity of equipment, software and procedures requires the definition of a standard for elaborating security documentation. This standard concerns, first of all, the presentation model and the content of the document: all the security elements are described according to the same model which thus facilitates the actions of authorized personnel regarding their use and their maintenance. Secondly, the standard concerns the manner of creating the documentation, that is to say, the writing, the printing and the classification of documents. In addition, all the elements having been used for the elaboration of the document are handled and protected in the same manner and conditions as the resulting security documents.
ACR-13: Production of documents by the organisation	Every document produced by the organisation must be in conformity with the graphical charter and its quality assurance policy. It must notably carry a unique reference, permitting to clearly identify the author, the creation date, elements of version control as well as mention of the document classification, figuring clearly in the document. The security of a piece of information is affected the moment it is published in a document. The creator of the document is by default the owner of it. He is also responsible for its classification. In function to the classification of the information, the media becomes subject to the application of the suitable rules of protection. Specific security rules will be applicable in function to the classification.
ACR-14 : Maintenance of security documentation	An organisation and rules must be stated so that all security documentation is up-dated upon completion of any modification (see documentation management) and that the old documentation is archived or destroyed.

3.3.6 ASH : Human aspects

ASH-01:	For employment positions that treat information relating to defence secrets,

Recognition of responsibility	signing an attestation of recognition of responsibility represents a personal engagement to respect the laws, regulations and security rules of the information system. The attestation is written and signed in conformity with IGI 1300. Specifically, article 16 stipulates: "...this attestation signifies that the nominee affirms to have understood the specific obligations and penalties imposed by articles 70 to 85 and R24 of the penal code upon any guardian or holder of information pertaining to national defence and state security [...] the managing director or manager directly responsible is charged with drawing the attention of the nominee to the implications of this attestation". For employment positions other than this category, specific clauses of confidentiality, employment termination and exclusivity can be included, if necessary, in the employment contract. The [REC 600] addresses these issues for information not covered in [IGI 1300], specifically that: "All categories of personnel required to have access to company information resources must firstly sign a responsibility engagement document (e.g. section 1.). This document may contain elements specific to each category of personnel." The application of penalties may be added to the essentially dissuasive character of this measure. In this case, disciplinary consequences for a failure to comply with internal security rules must be explained to new personnel from the start.
ASH-02: Security clauses in employment contracts	Employment contracts must: - either include explicit clauses for information system security such as: o prohibited actions o obligation to report anomalies or security failures, o duty of confidentiality, o clauses of confidentiality, o responsibility towards rules that protect company assets; - or make formal reference to the different rules that are applicable in the domain (e.g. chapter treating legislative and regulatory obligations), such as: o the PSSI, o codes of professional conduct, o organisational rules (charters, company regulations...). These elements must treat the sanctions or applicable measures in the case of a failure to comply with these engagements. Equally this principal must be extended to any placement or temporary work contract. Management personnel or personnel performing security-related tasks (security administration, inspectors...) must sign engagements specifically related to their duties. The different engagements, including those not integrated in employment contracts, must be reviewed and validated by the organisation' judicial service (e.g. previous chapter treating responsibilities. (e.g. Authorisation principles and e.g. Legal and regulatory obligations)
ASH-03: Adoption of selection criteria for personnel working on sensitive IS'	This rule concerns all categories of personnel working on sensitive information systems. It details, for all employment concerned with system operation and use, the mode of selection to apply for personnel recruitment and, particularly, required security criteria for each employment post. For example, requiring references for sensitive posts can be considered during hiring procedures. This rule implies the possibility of verifying work references of a candidate as well as those of a temporary employment candidate for an activity requiring the use of the information system.
ASH-04: General principals of authorisation	The IS must only be accessible, physically and logically, to the designated authorized individuals. Therefore, restrictions on access to information systems are defined according to their sensitivity (e.g. classification) and to the criticality of data and resources subject to these authorized actions Authorisations are assigned to a natural person and are not inheritable. Owners of a system or data decide on the assignment of authorisations. The allocation of authorisations must respect the principal of 'need to know': each

	party will have access only to the information he needs to accomplish his duties.It is recommended that the principal of least access (by default no authorisations) be applied upon the opening or launching of any new system.
ASH-05: Authorisation categories	Authorisation categories must be taken into account if the process of personnel recruitment or selecting suppliers uses an authorisation procedure. All authorisations must correspond to the restrictions placed on personnel: verifications and controls to perform (identity, competence), signatures for specific engagements...
ASH-06: Assignment and engagement rules (responsibilities)	The assignment of authorisations is determined at the moment of personnel recruitment. The time and the place must be fixed. The individual assigned the authorisation must formally recognise his knowledge of the responsibilities incumbent to the authorisation that he is allocated.All authorizations for a domain or an information system project must be formally authorized by the owner (manager of processing protection and information processed by the IS).
ASH-07: Personnel in reserve	Organisational measures can be taken to ensure that a vital post is never vacant, even temporarily (vacations...). The organisation should make provision so that for all vital posts there is a sufficient quantity of experienced personnel in reserve. All individuals holding a vital post should have a replacement at their disposal who has equivalent competence and similar knowledge of the dossier.
ASH-08: Authorisation procedure for sensitive posts	The sensitivity of a post refers to the need for confidentiality, to the availability and integrity of information, to the software and materials the post requires; this sensitivity is defined according to classification criteria (e.g. chapter treating information security), but can also be related to localisation issues: a post of human relations manager in a region with a high risk of social unrest can be considered as a sensitive post. For a post that includes the handling of defence secrecy information, authorisations for personnel are defined in article 3 of [IGI 1300]: The authorisation procedure consists of verifying that an individual can, without risk to defence secrecy, state security or the individual's own security, have knowledge of information subject to a given classification level in the exercise of his duties. At the end of the authorisation procedure, the competent authority decides to permit or not the individual concerned to have knowledge of the information of the requested classification level". For sensitive posts that don't use information relating to defence secrecy, an authorisation procedure can be used that models the one that must be applied in the context of the defence market. In this case, it is possible to refer to [REC 600].
ASH-09: Partitioning sensitive posts	Partitioning sensitive posts aims to prevent information leaks representing a risk for state or organisational interests. To preserve state interests and, particularly in the context of protecting defence secrets, decisions of admission to or approval of access to information of a certain classification level, such as is defined in the articles 10 to 12 of [IGI 1300], do not in themselves authorize the beneficiary to access all the information relevant to this level; the need to know this information remains a function of the activity of the individual or the particular dossiers that are conferred to him.In a similar manner, to protect the interests of an organisation whose information is not that of defence secrets, knowledge of the need of information to accomplish a mission or do business permits an efficient partitioning of posts.
ASH-10: Delegation	The owners or holders of information can delegate the implementation of protective measures to organisation personnel. However, they retain responsibility for security. Thus they must have the means at their disposal to control the respect of security rules. Authorisations are assigned to a natural person and are not inheritable.

3.3.7 PSS : Business continuity plans

PSS-01: Definition of the scope of a continuity plan	It is appropriate to precisely define the entire framework of the continuity plan (resources, responsibilities, test periodicity...) for each of the following aspects: - facilities, materials and information networks;

	- programs and information data; - information system users.An ISS risk analysis will provide the elements permitting a decision on the necessary plans for the organisation. These plans have a high cost that should be justified.
PSS-02: Application of external services	Continuity plan management which include external partners must be in-depth, notably during the phase of drawing up contracts. It must contain elements that are relative to regular testing with the aim of verifying the correct functioning of plans.
PSS-03: Preparation of a recovery plan	A plan for information recovery (or plan for the resumption of activity) is necessary to protect the critical operational tasks of the information system in the face of major failures, human error, natural disasters or deliberate attacks. The aim is to limit security leaks following a major incident and to return the information system to its initial state. A plan for the resumption of activity requires considering all the operational requirements of the information system to assure recovery to normal functioning. The procedures resulting from this plan provide an alternative and temporary means for service continuity in the case of damage or failure of equipment. However, an element fundamental to the establishment of a plan for the resumption of activity is the study of the information system's availability for the extent of the loss suffered is generally a function of the length of unavailability. Therefore the availability study aims to correspond different brackets of down time and their loss levels to the emergency procedure levels of the activity resumption plan.
PSS-04: Positioning of applications in the continuity plan	In function to the organisational risk analysis, each application must be ranked in terms of resumption of priority. This ranking corresponds to a measure of the impact that the unavailability of the application would have on the activity of the organisation.
PSS-05: Implementation of back-up procedures	A back-up plan taking into account the time required for rebuilding information by activity type and/or process must be put in place. A distinction is made between back-ups of system applications and data. To qualify for a high confidence level, the back-up plan must be tested regularly. The procedure of regular back-ups of vital data and software is a key measure, classically, a minimum number of information back-ups is stored in a location sufficiently far away from the main site to ensure their protection from a damage at the main site; physical protection of back-ups is at a similar level as the standards applied at the main site. Means of control of the consistency and the integrity of information back-ups must be implemented and managed.
PSS-06: Regular testing of plans	To qualify for a high confidence level, the continuity plan and associated plans must be tested regularly. At the end of each of these activities, a "feedback" group will be put in place who will updates plans after analysing failures or delays

3.3.8 INC : Incident management

INC-01: Definition of possible abnormal situations	The types of possible abnormal situations cover among other things: - failures or service faults of physical equipment; - failures or service faults of software and applications; - problems due to missing, incomplete or abnormal data inputs; - production of missing, incomplete or abnormal results; -... The risk analysis provides the elements to take into consideration in the choice of warnings to report. These choices are specifically linked to the selected security objectives.
INC-02: Implementation of a network for alerts/detection of security incidents	The goal of an alert network is to trigger action as quickly as possible, as soon as an incident is detected, thus to reduce the consequences of the information system stopping or to minimize the procedures activated following incident occurrence. All users, and particularly those working in sensitive posts, form the links in the chain of this alert network. The objective is to inform users on how to protect their

	material and how to identify the indications of illegal manipulation or unusual activity. The efficiency of an alert network depends upon the structure of the organisation implemented and, specifically, upon security officers. It depends on the technical level of detection methods and the efforts of information system users. The resulting actions are all the more efficient as they provide the appropriate means at the opportune moment. In the case of compromised defence secrecy information, the organisation must study a rapid response: "If information security has been or appears to have been compromised in any manner whatsoever, the speed and the discretion of the action takes on a particular importance so as to limit the consequences; a report that is unfounded and contradicted by the facts is always preferable to a delay in taking action.
INC-03: Control of security incidents	Control of security incidents consists of assuring the continuity of security throughout the action following an alert: recourse to specialists from the exterior and the obligation to provide them access to the information system site must not exempt personnel of the organisation from applying the security rules. This control is obtained by respecting pre-established procedures. Two emergency situations can necessitate different actions: - those originating from physical accidents affecting the infrastructure of a sensitive zone or the information system contained within and which do not lead to hostile actions aimed at capturing information system elements; the action consists then of surveying material, software and documents during the intervention like, for example, the transfer of equipment to a clean room or downgrading security mechanisms until the information system is returned to normal, - those originating from hostile actions aimed at capturing information system elements: a plan of emergency destruction that is simple and practical to employ can be, in certain cases, the only means of avoiding serious compromise.
INC-04: Security incident follow-up	The absence of a security incident follow-up exposes the organisation to a misunderstanding of the vulnerabilities of its information system and condemns it to be without the means to react efficiently to a repetition of similar damages. Because of this, responsibility and procedures for incident follow-up must be established; the procedures cover therefore all types of potential incidents including system failures or service interruptions, errors resulting from false or inadequate data, leaks of confidentiality. To accomplish this, security incident follow-up is based upon reports on immediate action, notes on malfunctioning for deferred actions and, in both cases, on the analysis and the identification of the causes of the damage and statistics that can be established on their occurrence. The adoption of a reporting standard and directives for their use are measures that seek to establish encompassing and compulsory procedures for the alert in question. Incidents of any nature, detected for example in an operational phase, are reported to the security management level as rapidly as possible. Information system malfunctions and weaknesses must be noted and corrected. In particular, it is necessary to review malfunctions to ensure that corrective measures have effectively been implemented and that they correspond to authorized actions. The analysis and identification of the causes of incidents imply planning for the collection of audit reports, implementing protective measures and communicating with the users affected by the incident.
INC-05: Means of detecting intruders or illegal use	It is recommended that devices and/or procedures can detect intrusion attempts or illegal use and thus permit, in response, taking the necessary measures to cause these attempts to fail. Thus for each component or sensitive application of the IS one should implement ad-hoc means, which can extend to a properly configured surveillance mechanism to specific tools like intrusion detection systems.
INC-06: Implementation of an efficient alert	The principal is to quickly determine the occurrence of an event that constitutes (or is likely to constitute) the beginning of an attack, a major incident or that stems from malicious intent.

service	The alert service must organise the relay and the centralisation of incident detections through the use of simple information processing (e.g. roles) and must increase user and manager awareness of the obligation to report each fault. One should make provision for several alert levels. These different levels must be detectable by users meaning that everyone must know at which level the IS is at a given moment.
INC-07: Prediction of instinctive responses in the face of emergency situations	The principal is to select typical damage scenarios and to formalize the best responses in terms of protective measures to limit, or even avoid, the impact of the incident or the attack spreading, and in terms of decision making power and internal and external information, if need be. The above helps prevent the incident to degenerate to a damage of detrimental or unmanageable consequences for the organisation Each alert level corresponds to a clear procedure of actions to take. This type of procedure relies on the principal of in-depth defence which allows establishing protection barriers that are independent and in function to the alert.

3.3.9 FOR : Awareness and training

FOR-01: Documentation of responsibilities	It is fundamental that all the responsibilities of the ISS be written in an unambiguous manner and communicated to the individuals responsible for it. The description of these responsibilities must include the limits in terms of time and space associated to each individual. It is equally essential that all concerned parties formally confirm knowledge of and accept these responsibilities.
FOR-02: General awareness to security	Stimulating awareness aims to have each user understands that he holds an important part of the responsibility in the fight against malicious activities. The definition of the objectives of this awareness campaign is tightly bound to the organisation's mission or business, to the sensitivity of information assets and physical assets, as well as to known threats. These objectives can be, for example, a desire to obtain the support of personnel in relation to organisational assets or even the emergence of and the efficiency of an alert network involving all information system users. An awareness campaign that does not address clearly expressed objectives merely provides the illusion of confidence in the capacity of personnel to react efficiently to a breach of the information system. An awareness campaign repeated at regular intervals must be planned and led by the group responsible for the ISS. The goal of this campaign is to reiterate the main messages of the organisation's ISS policy and specifically to remind each person of: - security risks; - principal threats; - laws, rules, charters; - security organisation; - the principals and the security rules of the organisation; - behaviour to adopt; - specific rules (roaming work stations, teleworking activities...)
FOR-03: Communication on the ISS	Information concerning organisation and general requirements of the ISS must be communicated to the largest extent within the organisation. A means of communication must thus be defined and known to all, which allows finding all the ISS related information of the organisation (procedures, contacts, ...). One means used can be, for example, the implementation of an intranet domain dedicated to security in the organisation. The global ISS policy must be known by all organisation personnel, the specific ISS policies must be made known to the personnel using these particular systems. The distribution of a part or the totality of the ISS policy to third parties accessing the information system must be in function to their need to know and must in every case be validated by the organisation in charge of the ISS (see ORG). An introductory document must be prepared to ensure that every new person accessing the IS is informed of the organisation, the security rules and of his obligations. In a similar manner, a departure document is prepared to inform

	personnel leaving the organisation of the procedures and rules to respect.
FOR-04: Implementation directives for the judicial protection of information of the organisation:	This rule aims to promote the awareness of personnel of the obligation of judicial protection of the information they use or are entrusted with so as to reduce the risk of misuse or appropriation by third parties. The implementation directives refer, in part, to the principal of responsibility of personnel and, more specifically, to the rule relative to the idea of responsibility-holder (see chapter on responsibility ORG).
FOR-05: Matching security awareness to different classes of users	In security matters, the levels of concern differ considerably according to whether they apply to managerial personnel or non-managerial personnel. As a consequence, security awareness is adapted to the levels of responsibility held and to the characteristics of the post. The personnel concerned belong to three broad categories: - one related to corporate activities, supervision, management, exterior relations..., - one related to information system employees (engineers and technicians, office software users...), - one related to the security of the information system (engineers and technicians of the security team, security officers...) for which specialist training is required. Security awareness that does not take into account the operational particularities of each user and the more or less strict requirements related to responsibilities or workstations does not meet the given objectives and leaves the impression that security is an additional restraint without added value with reference to the need for workstation productivity
FOR-06: Stimulating ongoing ISS awareness in personnel	The ongoing provision of information to individuals aims to obtain a constant level of vigilance. This information specifically concerns updates to the ISS policy and threats. It allows bringing information up to date, communicating new information and equally to issue reminders concerning the rules or instructions that are not being applied correctly. Each update concerning the organisation and general requirements of the ISS also must be communicated.
FOR-07: Stimulating awareness of how to handle incidents	Above and beyond basic operations, the personnel concerned must be made aware and trained to the level required concerning operational security aspects for which they are responsible.* One of the essential points of security obligations concerning operating tasks involves respecting requirements: - recordkeeping in an incident logbook, - notification/alert of the person in charge (see the following).
FOR-08: Preparation and training in crisis management	Other than to anticipate the possibilities of and the response to (procedures) anomalous situations and incidents (FOR-07), it is essential to prepare and train the personnel concerned, which especially implies: - the presentation of ad-hoc plans (rescue plans, continuity plans, recovery plans...), - personnel training through simulations (exercises comparable to a fire drill). (see Crisis management) A specific training program must exist for each officer profile to assure the correct reflex actions in case of an incident or a security alert.
FOR-09: Stimulating personnel awareness of the use of ICT	A personnel awareness campaign must be performed to deter the risks of external disclosure (voluntary or not) concerned with the use of information technology media and of communication (ICT), such as video, telephone, fax, voice... This particularly concerns verifying their intended recipient and being aware of eavesdropping, or other people nearby.
FOR-10: Personnel training for the use of TIC	This training will set out to present the responsibility of each individual in the domain of information engineering and communication (information and communication technology ... ICT) and to train each user in the use of information engineering and communication facilities, as well as the protective measures at his disposal.
FOR-11: Stimulating user awareness of the means of	The use of technical means to detect computer abuse or to maintain systems obliges the organisation to: - control information flows, - access "personal" resources,

supervision	- regulate exchanges and transfers (Network, Message handling, Internet) - retain elements of proof. It is to find a balance between control and respect for individual privacy and to avoid litigation, that is to say, to adversely affect the corporate identity of the organisation, that information control actions of parties in the information system must be inscribed. Thus it is recommended to draw up a regulatory charter that explains the objective, as well as the means of monitoring and gathering, of computer evidence.

3.3.10 EXP : Operational systems

EXP-01: Documentation of the rules and procedures for Operational systems	All activities of operational systems, eventually grouped into families, must be identified. Each procedure and operational rule of these activities must be precisely documented. This documentation could, according to requirements, result in several documents, each destined for a category of concerned parties in function to their role, responsibilities and need to know. It must be kept up to date.
EXP-02: Integration of the ISS in the rules and procedures for Operational systems	All operational system documents must include a chapter on security that has been validated by the organisation's security structure.
EXP-03: Separation of development and operational or production facilities	The separation of the tasks and the environment of development, acceptance tests and of other activities related to the workings of the information system (operations, system and network management, data entry, maintenance, security audit...) reduces the risk of deliberate or accidental misuse of system resources. This rule has an influence upon the level of security and upon the efficiency of the separation of duties and responsibilities; effectively it permits: - increasing security by reducing the risk of malicious or accidental modifications of programs thanks to the separation of duties related to, on one hand, an information system's operational function (requiring different resources), and on the other, access privileges to security-critical machine instructions. - improves efficiency by the fact that the accumulation of several technical functions may encourage an information professional from an operational team to perform "on the spot" debugging of software and disregard programming rules of which mention is made above (for example, not including comments in lines of code that have been modified). This separation of functions helps bring about a better demarcation of responsibilities in case of an incident.
EXP-04: Conditions on the use of facilities management	Distinction is made among different types of facilities management: outsourcing, remote services (including remote maintenance), on-site facilities management...The conditions on the use of facilities management must be carefully defined, and as far as possible, based upon a specific risk analysis. For example, generalising remote maintenance services permits optimising costs by reducing personnel off-site travel. However installing a communications line from the information system to the maintenance organisation and the need to give high level access rights increases the risk of information system attack. (see remote activities operations)
EXP-05: Security conditions for maintenance of elements of the IS	Non-compliance with the orders for the preparation of an element before placing it in maintenance can expose the organisation to the operation of the information system being compromised or damaged. Conditioning consists of preparing the element for its repair, that is to say, verifying the following points: - removal of non-volatile storage that contained classified or confidential information, - overwriting any remaining memory so as to prevent any interpretation possible of previously recorded data, - verifying that the external maintenance installation meets the same security

	standards for material and personnel as those applied in the zones used by the elements sent for repair. If for technical reasons it is not possible to remove non-volatile storage, it may be necessary to require that maintenance of elements be carried out in place by security-cleared personnel. It is equally essential to take into account the maintenance of security components.
EXP-06: Security conditions for collection after maintenance	Security conditions for putting elements back into operation after maintenance aims to uncover any eventual tampering with hardware or malfunctioning.As a consequence, conditions for putting elements back into operation can be enacted, for example: - in function to local conditions, to an evaluation of the threat and, in the case of computers, of the sensitivity of information in the memory, the element is subject to measures of detection when it is reintegrated in its security zone, - for the specific case of material conforming to the standard TEMPEST, any modification requires a re-verification of its anti-radiation capabilities.
EXP-07: Follow-up of maintenance operations on elements of the IS	This rule, which applies to all information system elements (material and software), is of major importance in the case of elements having a security function. A lack of follow-up to maintenance operations consequently leads to a lack of knowledge as to the readiness of elements to resume their functions: it can lead to having a confidence in them that is unjustified from a security perspective. The follow-up of maintenance operations requires having a complete and detailed register on all actions performed on components so that personnel know the new configurations and apply correct procedures. In addition, when the organisation disposes of an infocentre whose principal mission is user support, it is necessary to monitor that the same rules are applied to all operations it is charged with and particularly when its responsibilities involve installing software packages or when users request the installation of cards with electronic technology on company machines.
EXP-08: Management of externally provided services	To develop the information system, the use of externally provided contractors (duly authorized in the context of the defence market) requires a strict application of the rules previously stated above and a reinforced control of available resources (sensitive application programs and files, compilers, editors, technical documentation...). The decision to make sensitive resources available must be taken in relation to operational requirements and the availability of the information system. The responsibilities and procedures between the organisation and contractors must be clearly established to ensure correct accountability in the event of any eventual incidents. The recourse to contractors, when security of the information system is an affair of state or is a major organisational issue, must never drift into a situation of contracting out the responsibilities of facility management. (see outsourcing of services)
EXP-09: Integrating the ISS in facility management contracts	Facility management contracts and their annexes should include a chapter on the ISS which clearly specifies commitments of the contractor and all concerned contractor personnel. Notably they must specify very precisely: - the security requirements to which the contractor commits (which cannot be inferior to those in force internally); - control procedures with respect to these requirements; - assignment of specific responsibilities to ensure proficient coordination in case of an incident or an anomaly; - the possibility of a change in requirements and procedures... to conform to changes in the ISS policy or one of its operational versions... and the obligation on the part of the contractor to comply with these changes.
EXP-10: Security in external services	The decision to and the contracting out of external services must be preceded by an analysis of risks and issues for the organization. The following issues must also be taken into account: - the responsibility of the organisation and external service contractors must be clearly defined and be written in the contract; - the sharing of the resources supplied by contractors to meet the needs of

	several clients may not correspond to security objectives; - the facilities of the contractor's information system that interfaces with the organisation's information system are not necessarily suitable, nor consistent, or compatible, to implemented security measures; - the possibilities and the modalities of audit control on the part of the contract giver are often found to be inadequate, in particular, given contractual arrangements that have been finalised, or the practicality of an on-site intervention on the part of the contract giver; - the individuals using and handling the information system are not always known to the organisation, yet these individuals may also simultaneously be in contact with potential competitors, or with managers of competitors; - on a functional level, privileges granted contractors to accomplish their duties are, in general, particularly broad, in terms of security (see maintenance access protection), and can be used to penetrate the information system. Therefore, a risk analysis related to these issues must be performed so as to determine security measures and objectives to over the identified risks, in particular regarding contractual clauses, traceability and follow-up of operations carried out.
EXP-11: Anti-virus control of software and data before they become operational	Controls of software and data before they become operational principally aims to combat the threat of contamination by viruses. Precautions can be taken to prevent and detect introduction of fraudulent programs (viruses, worms, Trojan horses, logic bombs...). All media external to the organisation and, in particular, media of uncertain origin, are controlled. Implementing dedicated means of systematic monitoring constitutes a counter-measure to this threat. These means must be implemented in a manner that ensures that all information system entry points are controlled (internet, network, servers, work stations). System elements with strong security needs and contamination paths must also be identified and protected. The numerous means of acquiring files must be taken into account (floppy disks, optical disks, encoded attachments to electronic mail...). Additionally clear instructions must be communicated to users forbidding the installation of any software on their work station.
EXP-12: Security control of the information system while in operation	The control of security of the information system while in operation permits reducing the risk of an attack on the availability and the integrity of information and data. These controls are performed, for example, by verifying the use of resources authorized for processing. The first aspect of these controls concerns information system users. It is the responsibility of system and network engineers to ensure direct visual control: examination of on-going transactions, files that are on-line, connection attempts... The second aspect of these controls concerns computer specialists in the role of verifying the correct application of security procedures, for example: - respecting the sequence of planned operations, - correct file handling, - the use of authorized macros, - respecting instructions for error recovery or exceptional events.
EXP-13: Reducing vulnerabilities	More and more services are being offered on office networks, which permits the transit of all sorts of information with variable security needs A policy of security surveillance must be establish so as to follow the state of the art in this domain and to react in an appropriate manner when significant vulnerabilities in the off-the-shelf systems and applications used in the information system are discovered. Surveillance will be concerned with attack methods, vulnerabilities and security solutions.
EXP-14: Procedures of secure information and data operations	Data and associated media must inherit the similar level of protection as the source information. In function to their classification, information and data are subject to specific operations. Thus vital or sensitive data processing may require the implementation of special technical measures (for example, using fault survival systems or disk mirrors) or of special organisational measures (for example, rules on sensitive work station partitioning) to avoid data processing incidents.

	Nominative information must also be protected according to law. This rule, which affects secure operational procedures, is justified by the vulnerability of data as it passes through different states (processing, backup, transfer between media, storage, destruction...): thus security procedures and controls set out to ensure continuity and protection during these diverse operational states. Among the procedures to put into place, those concerning data backup and the destruction of classified media have a major impact on security. - Data back-up is concerned with maintaining data integrity and availability: it must be performed regularly and the medium stocked in areas of similar protection levels removed from the processing zone; back-up integrity tests guarantee service continuity. -The destruction of classified medium implies that the recorded data be erased or overwritten before the magnetic media is destroyed (magnetic tape, floppy disks, removable and fixed disks, disk-based memories...). - For defence secret data, in conformity with regulations currently in force, the coding of data for intermediate storing of the media concerned in the case of discontinuous processing can be foreseen.
EXP-15: Implementation of an organisation for the fight against malicious code	Implementing an organisation and an ISS policy against virus threats diminishes the risk of the loss of information integrity, availability and confidentiality. This organisation must contain the following entities: - anti-virus unit (Administration, operations, up-date...); - support unit;- crisis management; - surveillance organisation. In the fight against malicious code, it is vital to define the relationships among the different interveners, in particular concerning surveillance, parties intervening in crisis situations, and regarding tool and procedure up-dates. The definition of an organisation for the fight against malicious code should define in particular the organisation to implement and the roles and responsibilities of each party. It will equally be necessary to implement a technical architecture for the protection against viruses for all information system components (work stations, messaging service servers, internet servers, back-up servers, data servers...)
EXP-16: Security instructions regarding tele-activities	Tele-activities group all network and workstation operating activities performed off-site: back-up, remote desktop, remote application installation, remote error treatment, remote maintenance operations... Tele-activities access is a special case when it applies to user workstations that have been assigned to users. Indeed, the user must be guaranteed that he conserves control of his environment and that no activities regarding his files nor intervention in his sessions can occur without his prior consent, a consent which helps bring about a feeling of mutual confidence between network administrators and users.
EXP-17: Protection and use of the messaging service	Clear and simple rules must be issued to ensure confidence in the use of the electronic messaging service. Thus a list of technical and non-technical measures must be established to fight against: - propagation and execution of malicious code ; - interception of sensitive unencrypted information sent by electronic mail; - disinformation or spamming; - publication of illegal or defamatory information, or harassment; One should firstly define rules related to: - storage of the evidence of electronic exchanges; - the use of security means (authentication, signature encoding); - use of messaging off-site (see remote access); - overloading of messaging system.
EXP-18: Rules specific to access filtering	Filter rules could be implemented on routers, the firewall and messaging servers so as to restrict access to certain identified servers. Effectively all that is not explicitly authorized must be forbidden and access filtered. This principal also holds internally.
EXP-19:	Certain categories of information require adapted conditions for its conservation

Standards for the conservation and destruction of protected information	and destruction. As far as defence secrecy information is concerned, regulations stipulate the measures to take according to the classification level. For the other categories, the measures are adapted to the organisational environment and must remain consistent. In particular, preliminary control of good storage practices take on a fundamental aspect the moment the information is confided contractually to an organisation. Emergency destruction can, for certain organisations, take on major importance in exceptional circumstances (riots, civil war...) but, more often, specific standards can be adopted to eliminate obsolete information which retains a residual character of confidentiality. Furthermore, archiving documents on magnetic tape have legal restrictions in terms of the length of conservation and protection of the medium, according to the nature of the information concerned (accounting or fiscal information relative to personnel...).
EXP-20: Control of removable media before it becomes operational	This rule, related to the control of removable media, principally treats information confidentiality and concerns organisations treating sensitive defence secrecy information or information seen as strategic for their activities. A key measure preceding the control of removable media before its reuse in another protected installation consists of erasing recorded information by completely overwriting contents with numeric or alphanumeric characters. For information concerning defence secrecy, memory media keep the highest data classification category for which they've been used in their history (except in case of declassification). This principal can be applied to non-classified information that is particularly sensitive.
EXP-21: Media, sources of infection and risks of disclosure	Organisations are aware of the security measures of systems. However, the protection of removable media (floppy disc, tape back-up, lists, reports...) is often ignored, even though it contains organisational information. By media, it is meant any item containing information : predominantly computer media, paper-based media (lists, documentation, printed reports...). Media must be protected in conformity to the information classification rules they contain. Thus, in function to the classification, security rules must exist concerning the management, control, storage (against theft and destruction), transport and the disposal of media. Even though today the threat of viruses (malicious code) comes principally from public networks, the introduction of viruses by media remains an important problem (see fight against viruses). Specific rules exist concerning the entry/exit of computer media in a classified zone (management of media records, media contents...); (see continuity in the protection of information).
EXP-22: Disposal of media or exit of IT equipment	IT equipment contains media that contains data of the organisation. The entry and especially the exit of this media must be controlled. This data, as well the data held in any other media of the organisation, must be destroyed when donated or when scrapped, either by physical destruction of the media, or by secure logical erasure (multiple rewriting). Therefore the organisation must define destruction rules by media type and, where relevant, by classification level. In the case of paper-based media, the organisation can either install shredders, or centralize the media to destroy and entrust this task to specialist organisations (with commitment of destruction). In both cases, particular attention must be paid to the protection of media storage before its destruction.
EXP-23: Photocopying documents	Security directives must be set out to control photocopying in function to the classification of the document. These directives should take into account obligations related to photocopying that are subject to specific legislation.
EXP-24: Storing of information by the organisation	Security rules for storing information must be defined and respected by all personnel in function to the classification. Principally these rules aim to ensure the protection of information from any disclosure or from theft by non-authorized individuals or from modification.
EXP-25:	Security rules must be drawn up to control the type of information that can be

Connection of roaming work stations and PDA	stored on these units. Protective measures and/or controls must be implemented to ensure the respect of these rules. Their connection to the organisation's information system must have been authorized and must respect the ISS policy. Particular attention must be paid to avoid that these units serve as a link between the information system and a public network.

3.3.11 ENV : Physical and environmental aspects

ENV-01: Continuity in the management of physical assets	The management of physical assets is assured all during their life cycle: deployment phases, installation, operation, maintenance, scrapping and destruction. These assets can also change owners or become the responsibility of someone else, be placed in a different environment or be subject to a change of use (loan of materials for an exhibition, be re-affected in the context of a new project). The rule requires that the measures chosen offer continuous protection no matter what the evolution or changes in use of physical assets. This continuity of management is based upon a choice of classification (including, where relevant, a defence classification in terms of [IGI 900]), related to the monitoring of physical assets from their operational beginnings, during their evolution and up until their replacement. The principal measures resulting from this rule concern the inventory, asset tagging and specific physical protection measures that correspond to their state (on loan, maintenance...) or their classification: - an inventory of physical assets permits the identification of those that require protection, - the operation of tagging is a concrete measure of recognition that an element belongs to a given classification, - specific physical protection measures designate actions to take in function to the selected classification. For example, a computer tagged "Confidential" should be situated in a physical environment that is adapted to this level of protection, for example like a "restricted area".
ENV-02: Taking into account operational constraints of the organisation	The implementation of means and procedures for the security of physical equipment that do not take into account the operational constraints of the organisation can hinder operational tasks and cause a rejection of this security by personnel. It is therefore necessary to take operational constraints into consideration for the implementation of means and procedures for the security of physical equipment.
ENV-03: Completeness of measures for the security of physical equipment	The following different types of measures must be taken into account. Protective measures of physical assets seek to limit damage, principally with regards to availability, integrity and confidentiality. The absence of a universal solution capable of responding to any type of threat obliges the organisation to implement a range of measures susceptible to counteract a line of attack and to repair any damage caused. : measures of prevention, detection, reaction and recovery Preventive measures aim to reduce the probability of a damage occurring. They consist, for example, of drawing attention to the placement of certain locales or to the location of installations (tape libraries, records room, piping, rooms for the storage of dangerous goods) regarding the risk of fire or flooding or to survey the conformity of the use of materials. Detection measures aim to sound the alert at an intrusion attempt or the outbreak of a damage in the perimeter of the information system. They must also be able to localize this alert. These measures are implemented in critical areas by the installation of the means of detection and alert like, for example, heat sensors or surveillance cameras. Measures of reaction aim to fight against a declared damage so as to reduce its impact. These measures involve starting the action the organisation has anticipated like, for example, a fire fighting service.

	Measures of recovery aim to limit the consequences of damages and facilitate a return to normal functioning of the information system. They can involve the activation of back-up resources or by the deactivation of security functions like, for example, temporary suppression of physical access control in the context of the security operating in a degraded mode. For the range of damages feared by the organisation, the measures chosen must be graduated, so as to offer a sufficient level of resistance to counteract or attenuate the attack.
ENV-04: Isolation of sensitive or vital systems	To isolate sensitive or vital systems allows minimizing the exposure of assets to threats. Risks are thus reduced. In addition, this offers the possibility to better distribute security measures by reducing the costs of a global protection.
ENV-05: Suitability of the measures of physical security to asset types	Physical security measures must be applied to all sites. They aim firstly to protect personnel then to reduce risks of destruction or of disclosure which could damage, directly or indirectly, the vital interests of the company or the organisation. This rule indicates that the measures mentioned in the previous rule can be adapted according to the three categories of physical assets, that is, the infrastructure, the material and support equipment.
ENV-06: Protection against accidents and breakdowns	In installations containing vital equipment for the information system (without forgetting network infrastructure components), considering threats from the surrounding environment, anticipate measures : - to prevent water damage; detection and reaction - (the best is to avoid keeping equipment in installations at risk like rooms containing water pipes or situated in flood zones); - fire detection and extinction; - control and back-up of electric current (at the least, the elements of protection must guarantee electricity provision for a minimum delay so as to perform all the back-up operations necessary);- back-up of the telecommunications network (pay particular attention to the procedures of switchover to back-up lines in a situation of line interruption); - of air-conditioning and air purification (take into account the supply of consumables such as water, gas, filters, as well as anti-dust measures); - formalized procedures of response in case of damage or break-down (including during non-working hours); - emergency procedures. The control of the environment must take into account temperature, humidity, dust and vibration. One must also anticipate an emergency plan if damages that cannot be controlled occur. (see crisis management) All installed protective equipment must be regularly controlled. Controls (notably concerning fire prevention measures) are required in the regulations. It is strongly recommended to apply these controls to equipment for which they are not compulsory (for example, the detection of the presence of water).
ENV-07: Physical protection of cables and telecom networks	Telecom and computer cables must, as far as possible, be protected against all malicious access which could lead to eavesdropping (buried lines, hidden cables...). It is essential to guarantee the protection of the access to equipment and network terminals. The protection of access to cables and other network components (whether they are authorized or not) consists not only of preventing eavesdropping (and also of preventing active listening) but also to avoid that they become accidentally damaged.
ENV-08: Division of the infrastructure in security zones	The sites, buildings and locales which contain material or immaterial assets (information and their associated media, information system materials), and that house critical activities from a security viewpoint, must be controlled, particularly with regards to their access. A security zone is a zone in which permanent measures are in place to control the movement of personnel and materials, as well as to detect and prevent any

	outside listener. A division of the infrastructure in security zones facilitates the installation of appropriate measures, particularly concerning the control of movements of personnel by the granting of access rights specific to zones. These rights can be bound to work stations and to levels of responsibility.
ENV-09: Application of reception and visitor traffic procedures	Reception and visitor traffic procedures are generally established by the general security service. But, far from interfering with this service, each information system user is obliged to take charge of applying this rule in his own work zone or in the vicinity of his own work station. The agent responsible is effectively the one best placed to verify that the information assets with which he is entrusted remain undamaged. This rule can be likened to the rule recommending the division of the infrastructure in security zones, measure which greatly facilitates controlling visitor traffic.
ENV-10: Specific management of physical assets requiring protection	Management of physical assets requiring protection consists of adopting a classification or a typology, management measures for these assets and protective measures throughout the asset's lifetime. The principal to respect is to adapt these means of physical protection, like any security measure, to the value of the asset to protect, yet remain coherent with other security measures in application. Article 10 of [IGI 900] thus defines: "Any document, software program or equipment, which, by its integrity or its confidentiality, contributes to the security of an information system, receives the denomination ACSSI (Information Systems Security Controlled Articles) which indicates that its management and its protection must be ensured in conformity with ministerial orders relative to Information Systems Security Controlled Articles". For non-classified defence physical assets, the adoption of a typology allows regrouping them according to their nature and affectation. Classes of protection are established in function to the security requirement level, that is to say, to the criteria of confidentiality, integrity and availability attached to these asset, so as to guarantee their continuous surveillance. The adopted typology is specific to the mission or business, to the culture and constraints proper to the organisation.
ENV-11: Procedures of secure operation of off-site equipment	Off-site equipment, be it dedicated or carried outside its security zone (portable computers, portable material, printers, photocopiers, faxes...) are often used by reduced operatives or even solitary users. With no immediate support and without the use of the physical protection of the security zone, the probability of incident or security attack to equipment remains very high: indiscretion and computer abuse represents a major threat in the sense that verification instructions are more difficult to implement. Thus using equipment off-site requires specific measures adapted to the environment; in particular and, whenever possible, situate peripheral equipment in a supervised area. The case of portable computer merits particular attention. Indeed, with the increase in memory capacity and processing power, portables are used more and more often. However, they are exposed to a greater variation of threats than fixed material and their use increases the difficulty of the necessary controls regarding the back-up of information. Their portability and small size greatly increases the probability of loss or theft. As far as possible, processing on portable computers may only occur in the areas designated in function to the classification level of the protected information being processed. When material is taken off-site, the same procedure must be applied as for taking classified documents off-site.
ENV-12 : Protection de la documentation de sécurité	Security documentation must be protected from non-authorized access. Its protection is of the same level as the elements to which it pertains The following measures are suggested: - each manger-holder of security documentation must know the position of the documents he is responsible for and control their use; - handling of these documents can only be done by authorized personnel; - the documents are stored in secure areas; - distribution ordered by the security manager may be restricted to a minimum of individuals.
ENV-13:	The agent to whom the equipment will be assigned, even temporarily, will be

Protection of equipment against theft	responsible, upon attribution, for its protection by using consistent and suitable means. As far as possible, when the equipment owner must take the equipment off-site, it is recommended to only store on the equipment the information strictly necessary to accomplish the off-site mission, and if necessary, to carry information on external removable media. The risk of theft of portable computers being great even on-site, a frequent inventory and control of machines must be done.A specific procedure must be formalized to define actions to take by the equipment owner and by the organisation in case of equipment theft.
ENV-14: Protection of back-up media	Back-up media must be protected against the risks of destruction, disclosure and theft. Particular attention must be paid to these types of media because, by their nature, containing a part of the information held in a system, they constitute a target of choice on which to perform information theft and to destroy the capacity of the organisation to recover from an accident.
ENV-15: Protection of system documentation	The documentation of systems (network architecture, naming policy...) contain information which, if associated to other information (information on vulnerabilities...) constitute the vital elements of a successful attack. Their disclosure to the exterior can be the opportunity for certain individuals to carry out intrusion attempts. It is therefore essential to make sure these documents have a classification and to make sure their distribution to outside parties is controlled, including to suppliers.
ENV-16: Off-site use	The exit and use off-site of all computer equipment must have been authorised. Rules must be drawn up to restrict their use in public places or on other information systems. Their connection to the information system of a client or a partner must have been authorized by the other organisation, and its owner has to respect the ISS policy. Computer equipment must be protected so as to avoid all unauthorized access to information the equipment stores and processes.

3.3.12 AUT : Identification / authentication

AUT-01: Use of the same secret to access several services	The assurance levels of the means used to protect authentication secrets vary according to the applications and systems. It is of fundamental importance that users determine the robustness of authentication systems in order to use the same secret in systems with consistent protection (e.g. use of the same password for authentication on the operating system and various applications). An identical secret must only be used for services with equivalent assurance levels.
AUT-02: Combination of means of authentication	To access to the information system, users are required to give proof of their identity at the start of a session (and, in some cases, during a session) by providing an authentication element. Current authentication techniques are based on three means: - something that is known, e.g. passwords; - something that is owned, e.g. smart cards; - something that is characteristic of the user (fingerprints, retinal scan, dynamic signature, etc.). The combination of these three means provides full and effective authentication, but at a relatively high cost. Consequently, the responsibility owner must determine with the help of the security agent, which combinations of these three concepts are most suitable for his information subsystem or sensitive applications. The combination of at least two of these concepts is commonly called strong authentication. The choice of authentication based only on the concept of "something that is known" represents the minimum security profile for an information system; it is therefore necessary to opt for dynamic mechanisms such as single-use passwords or passwords that can only be used a limited number of times; in this case the mechanism used is an access counter which must be included in the

	protection effort. The mechanisms used therefore rely on authentication elements for which strict management must be planned.
AUT-03: Uniqueness of users' identity	Users' identity must be managed under the combined control of the system management and the security officer of a site or operational unit (security officer level). Unique (and unambiguous) identification of an access holder is fundamental in guaranteeing traceability of operations and diagnosis of a security flaw (see inspection and audit)
AUT-04: Granting and retrieving means of authentication	However sophisticated the technologies used to control accesses to an information system may be, the granting, use and management of these means still remain vital aspects of the system. The following rules must therefore be clearly formalised and scrupulously followed: - before a user is granted access he/she must give a formal undertaking to comply with the basic rules for protecting the means of access provided and the duty of reporting their theft (or a mere suspicion that the secret has been disclosed) (see Responsibilities, see Assignment of sensitive posts); - the means of access (password, smart card, etc.) must only be granted after establishing that no-one but their owner will know the secrets; - the manner in which a declaration of theft or loss of a secret is processed must guarantee that the user's identity cannot be usurped; - whenever personnel leave the organisation (or are transferred), all their access rights to the information system must be cancelled. The fact that two or more persons know, for example, the password for a user identity must be considered to be a breach of security unless it is planned for the purpose of providing continuity of system administration functions. If, exceptionally, the sharing of an identity and authentication element is unavoidable, special measures, such as the use of recorded sealed envelopes, must be developed to prevent any abusive or incorrect use.

3.3.13 CAL : Logical access control to assets

CAL-01: Devices and procedures to protect against intrusion	The architecture of communication infrastructures must include devices and procedures providing the adequate level of protection against intrusion. Access to the IS and its main resources (applications) must be controlled in order to protect against fraudulent access and intrusion. The means to be set up vary according to the security objective and may include measures such as firewalls and authentication and access control systems. After an analysis of the ISS risks including cataloguing of each potential target and possible means of access for attackers, suitable defensive measures must be set up to cover the identified security objectives.
CAL-02: Network partitioning and flow control	The purpose of network partitioning is: - to facilitate access control; - to provide better protection against intrusion; - to prevent information leaks: ? to networks or workstations inside the organisation, addressed to persons who have know need to know this information; ? to networks or workstations outside the organisation; ? by connection from outside the organisation using the bounce technique for example via a workstation connected simultaneously to an internal network of the organisation and a modem. Partitioning allows reserved zones - well-defined security perimeters - to be created according to the need to know. Such internal perimeters must be set up whenever an analysis identifies sensitive subassemblies or applications warranting a security policy, access control and private communications. Communications from inside a security perimeter to the outside must always transit via an appropriate device (firewall) monitoring compliance with the rules set for this perimeter. To achieve this, it is essential to have a documented boundary "flow matrix" indicating the communication concerned, its recipient, its

	sender, its content, and the applicable conditions. Network partitioning for the purpose of information flow monitoring is based on the access rights of users, functions and processes. One partitioning solution is to protect sensitive information during its transmission. The principle involves checking that the information transmitted has correct level of protection. Protection of sensitive information during its transmission is organised in a way that renders the various types of attack on the transmission network as ineffective as possible.This protection is organised so as to ensure that: - traffic is routed even under jamming or saturation conditions (which prevent or disturb the operation of the links); - all intrusion (i.e. introducing or changing messages in order to deceive) is prevented; - there is defence against interception (i.e. reception of unauthorised transmissions); - there is defence against traffic analysis (i.e. obtaining information from a traffic study).The standard means of protecting communication security are the use of encryption systems and the use of equipment protected against the transmission of compromising signals . Encryption is defined as all the cryptographic tools used to protect transmitted information by making it unintelligible to anyone who is not authorised to know it. Encryption can be carried out on messages or on transmission channels. The principle takes account of the fact that if the security measures corresponding to the required protection level necessitate cryptographic means, the use of these means is subject to the law and regulations and must be accompanied by organisational measures allowing their specific management.
CAL-03: Procedures for secure use of the organisation's telecommunication networks	Secure use of the organisation's telecommunication networks must not jeopardise the security measures taken at the infrastructure level (such as creating reserved zones), personnel (such as managing the need to know), security organisation or hardware and software resources. The need to define rules for using the organisation's telecommunication networks is all the greater if users' access possibilities are increased by interconnection of internal networks.Secure use of the telecommunication networks requires the setting up of functions and mechanisms designed to guarantee the security of data during their transmission. The following breakdown can be adopted: - authentication; - access control; - data confidentiality; - data integrity; - non-repudiation; -availability. Access control, included in these functions, requires on-going management and control measures covering, for example, the following aspects: - users' access to services for which they are authorised; - connection of isolated computers or computers outside the organisation to the information system; - separation of networks dedicated to specific domains; - routing of communications on authorised channels.
CAL-04: Organisation of information system accesses	The organisation must set out the rules and identify the technical standards required for controlling and managing information system accesses. These rules must define the assurance levels of the access control means for: - access to the local area network (intranet) and transversal services - mainly messaging and Internet services - from the organisation's sites; - where appropriate, access to a secure subnetwork; - access to the organisation's applications; - access from the outside to the organisation's transversal services, especially messaging;

	- access to the equipment connected to the local area network; - access from the organisation's workstations to other networks; from the organisation's site or off the site; - access to the information system by suppliers; - public or "guest" accesses. The following characteristics must be defined according to the sensitivity of the information and/or information system functions: - technology to be used (authentication algorithm, password tried more than once, etc.); - protection of secrets (password files managed by the systems or applications); - access assignment conditions (user's undertaking to comply with the basic rules of access protection); - robustness requirements concerning means of access and passwords - construction rules - frequency of changing passwords - history of non-reusable passwords; - period of validity of access assignment; - any authentication procedure for sensitive accesses or accesses using media that are not considered trustworthy (public networks) must guarantee that the authentication elements are not disclosed; - procedure in the event of repeated unsuccessful attempts to connect; - connection time limits; - procedure if a secret is declared as lost; measures preventing usurping of identity; - procedure for cancelling access when personnel leave or equipment is stolen. Special attention must be paid to protecting remote accesses to the information from outside the organisation's premises (Internet access, switched network access). This protection concerns especially session theft, disclosure of secrets, usurping of identity, deliberate saturation of access, etc. For each of these accesses, procedures must be written to define profiles (including network and application operator profiles) and the assignment and management of access rights (see Authorisation). It is strongly recommended to adhere to the principle of only assigning an access and privileges when they are necessary for performing a task.It is of fundamental importance to make users aware of the need to protect information and the means assigned to them for accessing the organisation's information system (the workstations are the main points of access to the information system).
CAL-05: Files containing passwords	As far as possible, files containing passwords (or secrets) must be banned or encrypted (for example, connection script).
CAL-06: Cancelling uncontrolled accesses to the information system	It is important to be able to control all accesses to the information system. Special attention must therefore be paid to the following types of access: - equipment connected to the information system which also has a direct public access (for example laptop computer connected to both a modem and the local area network); - unauthorised connection of a workstation to a physical network access point.
CAL-07: Assignment of service access privileges	Assignment of an access and the associated privileges must be validated by the owner(s) of the accessed systems so that it can be checked for compliance with the user's authorisation and the responsibility principles (separation of powers, least privilege). It is desirable to keep an inventory of accesses and privileges that have been authorised for sensitive services.
CAL-08: Protection of special access to the IS (maintenance access)	Maintenance accesses require high-level privileges on the systems. When they are used from outside the organisation (for example by service providers), it is essential to define means of reinforced protection against any malicious use and also means of traceability. Specific commitments of responsibility must be included in service provision contracts (see Service contract).
CAL-09:	To maintain control of access to the information system, it is essential to conduct

Verification of information system access lists	regular checks (and possibly also spot checks) of the access and privileges list. This check can be conducted by comparing the access inventory with the records of users' signed commitments and the personnel list. The checks can be intensified for access to sensitive information and/or functions. There must be a procedure setting out the actions to be taken if an anomaly is detected (for example, an apparently unjustifiable access, privileges that seem to be too high, etc.). These procedures must take into account the impacts on the information system if privileges are reduced.
CAL-10: Checking information system user privileges	It seems important to specify a rule for verifying the right to hold privileges. This verification must be independent of checks on secure operation, which concern the way in which these privileges are used. The purpose of the check, activated whenever a user attempts to use privileges on an information system resource, is to inhibit the action if it violates the security rules in force in the organisation. The measures arising from this rule can be based on the following aspects: - actions for which a privilege check needs to be made; - the measures to be taken if an action is attempted by someone without the appropriate right; - the exceptions to the privilege check and the conditions for validating them.
CAL-11: Application of the notion of information system user profile	To apply the notion of information system user profile, the data (or objects) must first be structured according to the organisation's functions or activities, as defined by the responsibility owner. The data handled by users are structured according to the applications that use them within the functional unit (for example, stock management for a procurements department), in the shared-resources context (for example, local networks), or during a mission or special activity requiring the partitioning of workstations. In the same way, the various personnel categories (or subjects) must be structured by defining information system user profiles specifying access privileges for read operations (display, printing) and processing privileges for write operations (creating, modifying, destroying) in the context of users' responsibilities or activities. Delegation rules must also be defined and formalised.
CAL-12: Administration of information system user privileges	A user has privileges authorising the use of information system resources according to the profile assigned to him/her. Administration of these privileges must ensure that they are fully compliant with the security rules in force. The criteria for applying this principle must be clearly set out and may, for example, be based on the following elements: - the user profiles subject to privilege administration; - the privileges existing between the various user profiles; - the persons qualified to grant or modify privileges; - the conditions to be met before any modification or granting of privileges; - user privileges that are incompatible with each other. The system manager and security officer must specifically check that the integrity of tables containing privileges is protected.
CAL-13: Locking work sessions	The workstations are the main entry points to the information system. Users must be made aware of the need to make their work environment inaccessible during their absence (locking the session, shutting down the workstation). To reinforce this measure and avoid negligence, it is strongly recommended to set up automatic work session protection measures that self-activate after a certain period of inactivity (automatic disconnection, locking, etc.).
CAL-14: Protection of the work environment	The list of actions of each user profile (administration, maintenance contractors, main user of the workstation, temporary user) must be drawn up and protected by access rights.

3.3.14 JRN : Logging

JRN-01: Means of logging intrusions or fraudulent use	The IS must include means (devices and/or procedures) for logging intrusions or fraudulent use. As it will not always be possible to "block" intrusion attempts in time, the principle

	of risk management must be applied by setting up logging and tracking mechanisms. If there is a successful or attempted intrusion the mechanisms must provide: - trace data allowing the causes and sources of the intrusion to be more easily identified (tracking back to the threat agents); - trace data that are reliable enough to be accepted, if necessary, by a judge as proof of intrusion (or attempted intrusion) or fraudulent use if a complaint is filed. Procedures must therefore be set up - with the necessary technical and human resources - concerning the use of tracking and logging to detect intrusions, even after the event, and gather the necessary items of proof. These elements will also be essential for restoring the system to its initial state.
JRN-02: Records of operations	In compliance with the "Principle of proportionality" and volume measurement arising from the recording of security trace data, it is of fundamental importance to define the trace data generation rules so that the required data are obtained. These rules may be influenced by the resources likely to be used for analysing these trace data. The definition and implementation of these logging systems must take into account legislative and regulatory constraints concerning personal information.
JRN-03: Constitution of proof	Elements of proof relating to the information system must be constituted according to the legislation and codes of practice in force so that it can be presented in court if necessary. In particular, this concerns: - compliance with the principle of proportionality and transparency; - the acceptability of the proof; - the quality and exhaustiveness of the proof; - respect of private life; - the quality of production of elements of proof and their storage prior to their submission.
JRN-04: Management of trace data	The management of security trace data includes several tasks that must be defined and organised: - secure remote collection of security trace data; - archiving of trace data; - deletion of files of obsolete trace data (obsolescence and archiving duration must be fixed); - filtering and analysis of trace data; - protection of trace data against any damage or unauthorised access; - alerting if major events are detected; - checking the integrity of tracing mechanisms; - procedure for analysing trace data: remembering that the person analysing the trace data must not be the network administrator; - destroying trace data after the legal expiry date.
JRN-05: Security alert	The rules for following up the detection of a security incident depend on the seriousness of the incident. Incident classification may determine the method of transmitting the alert, the persons receiving it, the speed and type of reaction (see Management of incidents and crises). As a general measure, any relevant security incident must be traced and the trace data must be usable (identification of the author, date, type of operation, target, etc.). The rules for logging and analysing a security incident depend on its classification.
JRN-06: Analysis of records of security control data	To allow secure operation of the information system, security control data must be recorded in an audit log used to check compliance with the security requirements. In particular, this concerns accesses to the information system by users, technicians or computer specialists. Although analysis of control data is a retrospective verification, it can nevertheless reveal unsuccessful attempts to penetrate the system, or more insidious preparation of an attack by retrieving files and expired accounts. This examination provides more information than real-time monitoring, provided that it is conducted regularly and thoroughly. Effective protection of the mechanisms used to record control data is an essential

	condition in justifying the trustworthiness of records analysis. Any intruder will first attempt to inhibit the recording mechanisms and delete the proof of his misdemeanour. The implementation of audit logs may be a constraint during periods of heavy operating load. Nevertheless it is essential to be aware of the security risk that arises if they are deactivated, especially the legal risk taken by the organisation if it is used as a bounce site in an attack.

3.3.15 IGC : Cryptographic key management infrastructures

IGC-01: Key management policy	The use of cryptographic keys in the context of a key management infrastructure requires a key management policy to be established, implemented, monitored and maintained. This policy generally takes the form of a certification policy and a declaration of certification procedures which formalise the requirements concerning key management. They pay special attention to the lifetime and replacement of keys. It is preferable that the structure and content of these documents comply with international standards (such as RFC 2527). It should also be noted that a certification policy is much easier to establish after conducting an ISS risk analysis and studying other certification policies dealing with the same type of need (server authentication, user authentication, signature, encryption, etc.).
IGC-02: Protection of secret or private keys	Users may be required to employ secret or private keys for various reasons: encryption for confidentiality, authentication or signature. The integrity and secrecy of these keys is of fundamental importance for the strength of the system in place. Specific attention must be given to this problem, checking that in every case the choices and means adopted are consistent with the issues at stake in the use of these keys. Documents classified as "sensitive" may, for example, be subject to the requirement that all encryption be carried out using a system guaranteeing that the private key is stored and used in a hardware device (such as a cryptographic smart card), whereas a software solution could be used for other purposes.
IGC-03: Certification of public keys	In an asymmetric cryptographic system, there is a risk of usurpation of the public key. The security system depends on the reliability of the key management infrastructure and especially on the certification process linking an element (person, server) to a public key. It is essential to control this aspect by writing a certification policy.

3.3.16 SCP : Compromising signals

SCP-01: Zoning	One of the means of protecting against compromising signals is zoning. Zoning covers two aspects: - zoning of the premises in compliance with Directive 495 of 19 September 1997, - zoning of equipment in compliance with Guide 430 of 1 June 1999. When the zoning results are available, the equipment must be installed in compliance with Directive 485 of 1 September 2000.
SCP-02: TEMPEST equipment	One of the means of protecting against compromising stray signals is the use of equipment compliant with the TEMPEST standard (Transient ElectroMagnetic Pulse Emanations Standard). This equipment is developed according to specific criteria for reducing the transmission of compromising stray signals through emission or conduction. There are 4 categories: - A (compliant with standard AMSG 720), - B (compliant with standard AMSG 788), - C (compliant with standard AMSG 784), - D not complying with any of the standards above. The equipment must be installed in compliance with Directive 485 of 1 September 2000. This solution should be considered when zoning does not meet the need.

SCP-03: Faraday cages	Another, more costly, means of protecting against compromising stray signals is to use a Faraday cage or room screening.
SCP-04: Intentional compromising signals	Wireless transmission systems used to transmit information become potential sources of compromising signals known as "intentional compromising signals". This concerns all wireless transmission systems including infrared, radio frequency, optical, etc. To protect against the transmission of intentional compromising signals, the DCSSI recommendations should be applied, and in most cases encryption and/or equipment and room zoning should be employed. In addition, personnel must be made aware of the risk of using this kind of equipment to transmit information.

3.4 Other requirements

3.4.1 CCS : Security instructions

CCS_SIN: Instructions to follow in case of damage	
CCS_SIN.1.1	The security instructions to be followed in case of damage shall be written clearly and legibly, in accordance with applicable standards.
CCS_SIN.1.2	The security instructions to be followed in case of damage shall be displayed at eye level in unobstructed locations, in accordance with applicable standards.
CCS_SIN.1.3	The security instructions to be followed in case of damage shall be displayed at multiple locations on the site, in particular at points of passage and any locations specifically concerned by the instructions (e.g. lifts, equipment liable to cause flooding, etc.).
CCS_SIN.1.4	Security instructions to be followed in case of damage shall be printed on eye-catching media.
CCS_SIN.2.1	The procedure for summoning emergency services (fire brigade, ambulance service, police, etc.) shall be clearly mentioned on the security instructions to be followed in case of damage.
CCS_SIN.2.2	The site evacuation procedure (evacuation route, assembly point, etc.) shall be clearly mentioned on the security instructions relating to damages requiring evacuation (fire, severe pollution, terrorist attack, etc.).
CCS_SIN.2.3	Security instructions shall specify the appropriate course of action (what to do if trapped in smoke, first aid for electrocution victims, emergency measures in response to flooding, how to protect equipment in case of damage, etc.).
CCS_SIN.3.1	The security instructions to be followed in case of damage shall be regularly reviewed, to ensure that they are current (review frequency to be determined according to circumstances, but at least every two years).
CCS_SIN.3.2	The manager responsible for reviewing the security instructions to be followed in case of damage shall be clearly identified.
CCS_SIN.3.3	The security instructions to be followed in case of damage shall be approved regularly by the emergency services (fire brigade, ambulance service, etc.).
CCS_SIN.3.4	All site employees shall be informed of any updates to the security instructions to be followed in case of damage.
CCS_SIN.3.5	Security instruction awareness campaigns and where necessary practical exercises (tests, evacuation drills, damage simulations, etc.) shall be organised regularly (frequency to be determined according to circumstances, but at least every two years).
CCS_CSP: Preventive security instructions	
CCS_CSP.1.1	Preventive security instructions (e.g. no smoking near inflammable materials) shall be written clearly and legibly.
CCS_CSP.1.2	Preventive security instructions shall be displayed at eye level in unobstructed locations.
CCS_CSP.1.3	Preventive security instructions shall be displayed in the locations concerned by the instructions.
CCS_CSP.1.4	Preventive security instructions shall be printed on eye-catching media.
CCS_CSP.2.1	Preventive security instructions shall be regularly reviewed, to ensure that they are current (review frequency to be determined according to circumstances, but at least every two years).
CCS_CSP.2.2	The preventive security instruction review manager shall be clearly identified.
CCS_CSP.2.3	All site employees shall be informed of any updates to preventive security instructions.
CCS_CSP.2.4	Contractors and visitors to the site shall be informed of preventive security

	instructions by their accompanying employee.
CCS_SSE: Security instructions for essential services	
CCS_SSE.1.1	Security instructions for essential services shall be written clearly and legibly.
CCS_SSE.1.2	Security instructions for essential services shall describe preventive measures for avoiding the loss of essential services (e.g. connecting equipment to the backup power supply).
CCS_SSE.1.3	Security instructions for essential services shall describe the procedures for raising the alert in case of incident (e.g. who to contact if the telephone line is cut).
CCS_SSE.1.4	Security instructions for essential services shall describe incident response measures (e.g. install a backup air conditioning unit).
CCS_SSE.1.5	Security instructions for essential services shall be reviewed regularly, to ensure that they are current.
CCS_SSE.1.6	The manager responsible for reviewing security instructions for essential services shall be clearly identified.
CCS_SSE.1.7	All site employees shall be informed of any updates to security instructions for essential services.
CCS_CSG: General security instructions	
CCS_CSG.1.1	Security instructions relating to proper use of hardware and media shall be produced and distributed to all potential users.
CCS_CSG.1.2	Proper-use security instructions shall specify any practices that should be avoided (no smoking, eating or drinking near hardware; warnings relating to the saturation of data storage media or processing resources, etc.)
CCS_CSG.1.3	Proper-use security instructions shall specify any preventive measures to be taken (protection during transport, storage conditions, etc.).
CCS_CSG.1.4	Proper-use security instructions shall include guidelines relating to the operating environment of information processing facilities (temperature, humidity, etc.).
CCS_CSG.1.5	Proper-use security instructions shall be reviewed regularly, to ensure that they are current.
CCS_CSG.1.6	The manager responsible for reviewing proper-use security instructions shall be clearly identified.
CCS_CSG.1.7	All site employees shall be informed of any updates to proper-use security instructions.
CCS_CHI: Information system charter	
CCS_CHI.1.1	All internal and third-party users of the information system shall agree to abide by the proper-use instructions by signing an information system charter based on the proper-use security instructions.
CCS_SRI: Security aspects of internal regulations	
CCS_SRI.1.1	Security responsibilities relating to the information system shall be stated in internal regulations.
CCS_RGI: General installation rules	
CCS_RGI.1.1	General rules based on manufacturers' recommendations and the identified security sensitivities shall be drawn up for hardware installation operations.

3.4.2 CRR : Residual risks

CRR_ETU: Residual risk studies	
CRR_ETU.1.1	A residual risk study shall be conducted and regularly updated in order to determine the risks covered, the risks to be covered and the residual risks.
CRR_ETU.1.2	The identified residual risks shall be evaluated in terms of feasibility and probability as well as in terms of their impact (including financial, business, organisational and human impacts, etc.).

CRR_ETU.2.1	An action plan shall be produced for each residual risk, in order to mitigate direct impacts and minimise indirect impacts and edge effects if the risk materialises.
CRR_ETU.2.2	Wherever possible, residual risks shall be covered by relevant insurance (provided an appropriate policy exists at a reasonable cost).
CRR_SEN: Residual risk awareness	
CRR_SEN.1.1	Awareness of residual risks and the measures to reduce their probability/feasibility and impact shall be promoted among the organisation's employees.
CRR_SEN.1.2	The organisation's employees shall receive training in the action plans to be implemented a residual risk materialises.

3.4.3 CIS : Site installation instructions

CIS_PSI: Physical security chapter of the security policy	
CIS_PSI.1.1	The security policy shall include a chapter on physical security at sites.
CIS_PSI.1.2	The security policy chapter on physical site security shall state the applicable site installation standards.
CIS_PSI.1.3	The site installation standards shall include damage protection and impact mitigation measures.
CIS_CSI: Site installation instructions	
CIS_CSI.1.1	Site installation standards shall be based on applicable national and/or international damage (fire, accident, etc.) protection standards.
CIS_CSI.1.2	Site installation standards shall specify a physical zoning system capable of mitigating damage impacts (e.g. by isolating areas with fire doors).
CIS_CSI.1.3	The emergency services (fire brigade, ambulance service, etc.) shall regularly check that site installation standards comply with applicable national and/or international damage protection standards.
CIS_CSI.2.1	Premises (particularly at older sites) shall be audited regularly to ensure that they continue to comply with current installation standards.
CIS_CSI.2.2	Site evaluators and their replacements shall be clearly identified.
CIS_CSI.2.3	Site evaluators and their replacements shall be made aware of site protection issues and trained in installation standards.
CIS_CSI.2.4	Site compliance audits shall be documented in a detailed report submitted to management.
CIS_CSI.2.5	Site compliance audit reports shall be stored, processed and managed in the same way as other information system security records.
CIS_CDL: Construction of premises	
CIS_CDL.1.1	When building and fitting out premises, appropriate allowance shall be made for any unavoidable major risks (storms, hurricanes, earthquakes, etc.).
CIS_ADL: Fitting-out of premises	
CIS_ADL.1.1	Tinted windows shall be installed in any premises overlooked by another building.
CIS_ADL.1.2	Windows onto public thoroughfares shall be prevented from offering easy access to the premises by fitting security bars, toughened glass, restricted-opening windows, alarms that are triggered when windows are left open outside site opening hours, etc.
CIS_ADL.2.1	Premises shall be fitted out with due consideration for the items to be installed in them (temperature control, humidity monitoring, dust filters or other contaminant filters, etc.).
CIS_ADL.2.2	Equipment shall be installed as far as possible from any items liable to damage them (water pipes, heat or electromagnetic radiation sources, etc.).
CIS_ADL.2.3	Service rooms shall be spacious enough to allow facilities to be organised clearly and not interfere with hardware operation.

CIS_ADL.3.1	Standard items (network cables, water stopcocks, fuses, etc.) shall be marked so that users can locate them and identify their purpose.
CIS_SSI: Choice of site location	
CIS_SSI.1.1	The proximity of emergency services shall be taken into account when selecting a site location.
CIS_SSI.1.2	When selecting a site's location, due consideration shall be given to the risks inherent to the location (flood plain, proximity of vulnerable industrial facilities, pollution, etc.).
CIS_SSI.1.3	When selecting a site's location, due consideration shall be given to the potential for destruction by external events (collisions, terrorist attacks, etc.).
CIS_SSI.1.4	When selecting a site's location, due consideration shall be given to the risks of reduced employee availability (poor public transport services, easily blockaded site, etc.).
CIS_MPP: Protection measures	
CIS_MPP.1.1	Essential services supplies shall be fitted with clearly-identified, accessible cut-off devices (including a master cut-off device).
CIS_MPP.1.2	Cut-off devices for essential services supplies and any item that could be used to shut down essential services shall be protected against unauthorised access.
CIS_MPP.1.3	Wherever possible, any items that can be used to shut down essential services shall be located on-site.
CIS_MPP.2.1	Premises shall be equipped with fire detection and fire-fighting systems.
CIS_MPP.2.2	Fire detection and fire-fighting systems shall be adequately sized and appropriate to the sites and areas where they are located.
CIS_MPP.3.1	Sites liable to severe flooding shall be equipped accordingly (sumps, pumps, etc.).
CIS_MPP.3.2	Any areas particularly sensitive to flooding (electrical equipment, paper archives, etc.) shall be equipped with suitable sensors.
CIS_MPP.3.3	Any points of contact with the exterior (ceilings, windows, etc.) shall be watertight and inspected regularly to ensure that they remain watertight.
CIS_MPP.3.4	Special flood protection measures shall be installed at facilities in locations prone to flooding.
CIS_ZOS: Security zones	
CIS_ZOS.1.1	Organisations shall implement security perimeters to protect the areas containing production equipment or essential services distribution equipment.

3.4.4 CRI : Relations between sites

CRI_MOF: Control of dependent organisations	
CRI_MOF.1.1	Sites belonging to the organisation shall undertake to abide by the provisions in the security policy.
CRI_MOF.2.1	Any major changes affecting a site belonging to the organisation shall be recorded in an installation report, to be submitted to the organisation's security manager (original site layout, changes to network connections, etc.).

3.4.5 CET : Management of third parties (example AEV)

CET_EGT: General management of third parties	
CET_EGT.1.1	Contractors and visitors to the site shall not be able to enter or leave the facility other than via reception.
CET_EGT.1.10	When a third party leaves the site, the accompanying employee shall submit any equipment or media reception and delivery receipts at the reception desk, in person.
CET_EGT.1.2	Wherever possible, visits by third parties shall be notified in advance, and

	reception personnel provided with a list of names of all visitors expected each day, together with the scheduled arrival and departure times of the accompanying employee.
CET_EGT.1.3	All visitors shall be authenticated upon arrival by presenting an official identity document; a visitor's badge shall be provided in exchange for the aforementioned ID.
CET_EGT.1.4	With scheduled visits, each visitor's name shall be checked against the day's visitor list. Any names not already in the list shall be added to it.
CET_EGT.1.5	Each visitor's arrival and departure times shall be logged.
CET_EGT.1.6	Each visitor's name, arrival time, departure time and accompanying employee shall be stored, processed and managed in the same way as other information system security records.
CET_EGT.1.7	An accompanying employee shall be assigned for every visitor on unscheduled visits, and the visitor shall not be allowed to enter premises without their accompanying employee.
CET_EGT.1.8	If a third party brings equipment or media to the premises, an accurate list of the items brought shall be compiled and kept with the third party's ID card; wherever possible, such equipment shall be marked as being off-site equipment.
CET_EGT.1.9	Any third party that brings equipment or media to the site shall leave the premises with the same equipment, or a signed receipt for each additional or missing item.
CET_EGT.2.1	A visitor's accompanying employee shall be contacted as soon as the visitor arrives.
CET_EGT.2.2	A visitor's accompanying employee assumes responsibility for the visitor at the reception desk.
CET_EGT.2.3	The accompanying employee is responsible for their visitor from the time they leave reception together until the visitor leaves the site. In particular, the accompanying employee shall ensure that the visit is conducted in accordance with the security principles specified in the security policy.
CET_EGT.3.1	Access by visitors to a site or zone subject to specific security sensitivities shall not be granted unless their authorisations have been verified.
CET_EGT.3.2	With external visitors, the visitor's accompanying employee shall have the appropriate authorisations.
CET_EGT.3.3	With employees from within the organisation, the employee's authorisations shall be checked at the site or zone's reception desk.
CET_EGT.3.4	Authorisations may be verified either by manually consulting the Authorisations base after authenticating a visitor or employee by means of their proof of identity, or else using an automatic authentication solution (e.g. using personalised badges).
CET_EGT.3.5	If an automatic authorisation verification system is used, the identification data and the date and time of entry shall be stored, processed and managed in the same way as other information system security records.
CET_EIP: Contractor management	
CET_EIP.1.1	All contractors working on the information system shall be informed of the security instructions before they begin work.
CET_EIP.1.2	An external contractor's accompanying employee is responsible for all actions performed by that contractor in the course of their work (technical intervention, compliance with instructions and the security policy, in particular relating to data protection).
CET_EIP.1.3	Interventions shall be closed by an intervention acceptance procedure that inspects the operations performed and the results obtained.
CET_EIP.1.4	Intervention acceptance reports shall state the contractor's name and company, the date and time of the intervention, the operations performed, the results obtained, any problems and the name of the accompanying employee.

CET_EIP.1.5	Intervention acceptance reports shall be signed by the contractor(s), the accompanying employee and by the intervention acceptance manager if different from the accompanying employee.
CET_EIP.1.6	Intervention acceptance reports shall be stored, used and managed in the same way as other information system security records.
CET_PLD: Management of long-term on-site services	
CET_PLD.1.1	Once the initial reception procedure has been accomplished, it shall be possible to treat an on-site contractor as a temporary employee of the organisation (with an access badge, information system access rights in keeping with the nature of the service, etc.).
CET_PLD.1.2	Any item supplied to an on-site contractor for the purpose of their mission (access badge, login and password, etc.) shall be identified and listed in an inventory of items supplied to the contractor, stating the date on which it was provided.
CET_PLD.1.3	The list of items supplied to an on-site contractor shall be stored, used and managed in the same way as other information system security records.
CET_PLD.1.4	The security instructions and security policy shall be provided to all contractors at the start of their service.
CET_PLD.1.5	Before beginning their service, all on-site contractors shall agree to comply with the security instructions and the provisions of the security policy.
CET_PLD.1.6	Before beginning their service, all on-site contractors shall sign an official confidentiality agreement.
CET_PLD.2.1	At the end of their service, all on-site contractors shall return all physical items (e.g. access badges) provided for the purpose of their mission.
CET_PLD.2.2	The act of returning the items provided to an on-site contractor shall be recorded in a Returned Items report, to be dated and signed by the contractor and by a manager from the organisation.
CET_PLD.2.3	At the end of an on-site service, all logical items (e.g. login and password details) assigned to a contractor for the purpose of their mission shall be disabled or destroyed.
CET_PLD.2.4	The act of disabling or destroying the logical items assigned to a contractor for the purpose of their mission shall be recorded in a Disablement/Destruction report, to be dated and signed by the manager responsible for the operation.
CET_PLD.2.5	Reports produced at the end of a service shall be stored, used and managed in the same way as other information system security records.

3.4.6 CGS : Security management

CGS_GMP: Password management	
CGS_GMP.1.1	The password policy shall require users to periodically change their password.
CGS_GMP.1.2	Passwords shall be entered away from prying eyes.
CGS_GMP.1.3	Users shall be made aware of good security practices when selecting and using passwords.
CGS_SVG: Backups	
CGS_SVG.1.1	The security policy shall include a backup policy.
CGS_SVG.1.2	All electronic documents shall be covered in the backup policy.
CGS_SVG.1.3	The data that must be backed up shall be identified in specific backup procedures.
CGS_SVG.1.4	Backup procedures shall specify the backup methods and resources, which media to use, the backup frequency and the procedures for managing blank and recorded media.
CGS_SVG.1.5	The managers responsible for each backup operation and their replacements shall be clearly identified.

CGS_SVG.1.6	Data backup managers and their replacements shall receive training in backup operations.
CGS_SVG.1.7	The backup policy shall be regularly reviewed, with a view to adapting it for any information system evolutions while maintaining backward compatibility with existing backups.
CGS_SVG.1.8	Backup procedure review managers shall be clearly identified.
CGS_SVG.1.9	Backup managers and their replacements shall be notified of any changes to backup procedures.
CGS_SVG.2.1	Backups shall receive the same degree of protection as the backed-up data.
CGS_ARC: Archiving	
CGS_ARC.1.1	An expression of needs shall be produced, specifying the required storage period and media reliability, for all data that must be archived.
CGS_ARC.1.2	The storage measures used to archive data shall comply with the archiving requirements stipulated for the data in question.
CGS_ARC.1.3	Data that must be archived shall be identified in specific archiving procedures.
CGS_ARC.1.4	Archiving procedures shall specify the archiving methods and resources, which media to use, the archiving frequency and the procedures for managing blank and recorded archive media.
CGS_ARC.1.5	The managers responsible for each archiving operation and their replacements shall be clearly identified.
CGS_ARC.1.6	Archiving managers and their replacements shall receive training in archiving operations.
CGS_ARC.1.7	Archiving procedures shall be regularly reviewed, with a view to adapting them for any changes in archiving requirements while maintaining backward compatibility with existing archives.
CGS_ARC.1.8	Archiving procedure review managers shall be clearly identified.
CGS_ARC.1.9	Archiving managers and their replacements shall be notified of any changes to archiving procedures.
CGS_ARC.2.1	Archives shall receive the same degree of protection as the archived data.
CGS_PPS: Workstation protection	
CGS_PPS.1.1	The protection features in the BIOS that prevent booting from removable media shall be enabled.
CGS_PPS.1.2	Unused computing services, functions and interfaces shall be disabled.
CGS_PPS.1.3	Computing services, functions and interfaces that are only used occasionally shall be disabled when not in use.
CGS_PPS.2.1	Only authorised personnel shall be able to modify the system or installed software.
CGS_PPS.2.2	Software shall be configured with due consideration for security aspects.
CGS_PPS.2.3	The software used shall be widely-used products, or have been audited.
CGS_PPS.2.4	The software shall be free of known security vulnerabilities.
CGS_PPS.2.5	The integrity of software code shall be protected against unauthorised modifications.
CGS_PPS.3.1	Hardware shall be protected against theft (restraining cables, security etching, etc.).
CGS_PPS.3.2	Removable media shall be catalogued and protected against theft and unauthorised access (storage in a locked cabinet to which only approved personnel have keys, restricted access to computer rooms, etc.).
CGS_GLI: Licence management	
CGS_GLI.1.1	A licence management system shall be introduced at operational level.
CGS_GLI.1.2	Licence numbers shall be backed up separately.
CGS_GLI.1.3	Licence agreements shall be stored in a place protected from fire and other

	damages liable to render them unusable.
CGS_GLI.1.4	Access to licences shall be restricted to authorised employees.
CGS_GLI.2.1	Access to installable versions of software shall be restricted to authorised employees.
CGS_OML: Proof of origin of hardware and software	
CGS_OML.1.1	It shall be possible to prove the origin of facilities, hardware and software, and their updates.
CGS_OML.1.2	Any certifications relating to facilities, hardware and software, and their updates, shall be verified.
CGS_OML.1.3	Measures shall be taken to ensure the authenticity of software code.
CGS_GMA: Maintenance management	
CGS_GMA.1.1	The facilities, hardware and software in the information system, as well as those designed to protect the information system and the provision of essential services, shall be regularly maintained and tested.
CGS_GMA.1.2	Maintenance and operational testing of information system elements, security elements and elements providing essential services shall be conducted in accordance with manufacturers' recommendations and applicable standards.
CGS_GMA.2.1	With internal maintenance, maintenance managers and their replacements shall be trained in maintenance operations on the facilities, hardware and/or software for which they are responsible.
CGS_GMA.2.2	With internal maintenance, the relevant technical documentation for the facilities, hardware and/or software to be maintained shall be available to maintenance managers and accessible to their replacements.
CGS_GMA.3.1	With third-party maintenance, a maintenance monitoring manager shall be appointed for each element (facility, hardware, software, etc.).
CGS_GMA.3.2	With third-party maintenance, the maintenance monitoring manager shall ensure that maintenance operations are performed at the contractually-agreed frequency.
CGS_GMA.3.3	With third-party maintenance, the maintenance monitoring manager shall ensure that an appropriate maintenance contract is in force at all times for each element for which they are responsible (by renewing contracts or taking out new ones).
CGS_GMA.4.1	The resources required for system and hardware maintenance shall receive the same level of protection as the maintained systems and hardware.
CGS_GMA.5.1	The budget allocated to maintenance shall be adequate to ensure quality maintenance for all hardware and software in the information system.
CGS_GMA.6.1	Upgrade maintenance operations shall always include a rollback procedure, as protection against any anomalies that may occur during a system evolution.
CGS_GSU: Support management	
CGS_GSU.1.1	CGS_GSU.1.1 Support services shall be available for facilities, hardware and software that are part of the information system or protect the information system.
CGS_GSU.1.2	The procedure for the provision of support services shall be known to information system users, or at least to the relevant incident management personnel.
CGS_GSU.1.3	If employees need to use the organisation's information system while off-site, the support services shall also be remotely accessible, including, where applicable, from countries with significant time zone differentials.
CGS_GSU.2.1	With internal support, support managers and their replacements shall have received thorough training relating to the facilities, hardware and/or software for which they are responsible.
CGS_GSU.2.2	With internal support, the relevant technical documentation for the facilities, hardware and/or software for which support is being provided shall be available to support managers and accessible to their replacements.
CGS_GSU.2.3	With internal support for simple elements, support may also be provided by the relevant incident management personnel.

CGS_GSU.3.1	With third-party support, a support monitoring manager from the relevant incident management department shall be appointed for each element (facility, hardware, software, etc.).
CGS_GSU.3.2	With third-party support, the support monitoring manager is responsible for contacts with the third-party support service in accordance with the procedures defined in the support contract.
CGS_GSU.3.3	With third-party support, the support monitoring manager shall ensure that an appropriate support contract is in force at all times for each element for which they are responsible (by renewing contracts or taking out new ones).
CGS_GDH: Authorisation management	
CGS_GDH.1.1	Users shall be authorised to consult and/or modify data or information system elements according to their need to know and/or modify such items, but not on the basis of their seniority within the organisation.
CGS_GDH.1.2	A user authorisations procedure shall be developed, to verify each user's need to know or modify data or information system elements before such authorisations are assigned.
CGS_GDH.1.3	The various types of authorisation shall relate directly to the security sensitivities identified for the organisation's infrastructure and information.
CGS_GDH.1.4	The various types of authorisation shall relate directly to the security sensitivities identified for the organisation's infrastructure and information.
CGS_GDH.1.5	The authorisation assignment managers shall be clearly identified according to the elements concerned by the authorisations.
CGS_GDH.1.6	Authorisation types and the authorisations granted shall be regularly reviewed, to ensure that they are consistent with the needs of the information system.
CGS_GDH.1.7	Responsibility for reviewing authorisations shall not be entrusted to authorisation assignment managers.
CGS_GDH.1.8	Authorisation files (containing the applicant user's ID, the authorisations assigned, etc.) shall be dated and archived when they have been processed.
CGS_GDH.1.9	Archived authorisation files shall be treated as sensitive information and protected accordingly.
CGS_GDH.2.1	The assignments associated with each authorisation shall be clearly defined.
CGS_GDH.2.2	When a user obtains a authorisation, they shall be notified of the associated assignments.
CGS_PDI: Infrastructure protection	
CGS_PDI.1.1	The security policy shall list the types of provision that must be implemented in order to protect the organisation's data processing infrastructure.
CGS_CIR: Classification of and responsibility for information	
CGS_CIR.1.1	The types of information classification used for the organisation shall be described in the security policy.
CGS_CIR.1.2	The security provisions associated with each type of classification shall be described in the security policy.
CGS_CIR.1.3	The security policy shall describe the responsibilities for enforcing the security provisions associated with each type of classification according to how the data is used.
CGS_PAI: Information access privileges	
CGS_PAI.1.1	The managers responsible for defining, implementing and controlling access to information shall be clearly identified.
CGS_PAI.1.2	Information access controls shall be regularly reviewed, to ensure that they are consistent with security sensitivities.
CGS_PAI.1.3	All potential users of systems affected by changes to information access controls shall be notified of the change.
CGS_PAI.1.4	The access privileges management procedure shall be as unobtrusive and as comprehensive as possible, to avoid hampering legitimate access to data or

	encouraging the "loan" of means of access.
CGS_PAI.2.1	All the assignable rights shall be defined in a specific regulation.
CGS_PAI.2.2	The regulation that defines the user rights shall give a clear definition of the rights used, and in particular the right to know and modify other rights.
CGS_PAI.2.3	The regulation that defines user rights the shall include indications for using these rights in terms of access controls and authorisations.
CGS_REC: Acceptance	
CGS_REC.1.1	Software acceptance and operational tests shall be performed on all platforms on which the software is liable to be installed.
CGS_GPC: Critical process management	
CGS_GPC.1.1	As far as possible, critical processes shall be hosted by the central organisation.
CGS_GPC.1.2	If a critical process must be delocalised away from the central organisation, measures (activity reports, remote administration, etc.) shall be implemented to enable the central organisation to control the process.
CGS_GPC.2.1	It shall not be possible for a single individual to run critical processes.
CGS_GPC.2.2	The results of critical processes shall be validated before they are used.
CGS_GPC.2.3	Critical processes shall be validated by at least two managers within the organisation.
CGS_GPC.2.4	The managers responsible for approving critical processes, and their replacements, shall be clearly identified.
CGS_PEP: Protection of shared spaces	
CGS_PEP.1.1	Spaces intended for information exchange or sharing shall be protected against unauthorised access in the same way as the other spaces in the information system (authorisations, access rights, authentication, etc.).
CGS_OES: Organisation and security	
CGS_OES.1.1	The organisational structures implemented within the entity, and between it and its partners, shall facilitate the identification of individual users.
CGS_OES.1.2	Any organisational changes introduced as a consequence of a change in organisational strategy or policy shall not reduce the scope of the risks covered.
CGS_OES.1.3	The transitional periods involved with organisational changes shall be planned, and shall not allow access rights and assignments to overlap.
CGS_HSI: Non-information system security protection	
CGS_HSI.1.1	Security devices that are not part of the information system (smoke detectors, flood detection mechanisms, lightning conductors, etc.) shall be protected in the same way as equipment that is part of the information system.
CGS_HSI.1.2	The organisation's personnel shall be made aware of the need to protect non-information system security equipment.
CGS_GSS: Backup system management	
CGS_GSS.1.1	At their simplest, backup mechanisms shall consist of redundant devices with sufficient capacity to satisfactorily provide any services identified as being of strategic importance.
CGS_GSS.1.2	The sizing of redundant backup equipment shall be reviewed regularly, and at every major information system upgrade, to ensure that it remains appropriate.
CGS_GSS.1.3	All backup (whether redundant or otherwise) systems shall be sized to provide quality of service consistent with the objectives identified for degraded-mode backup solutions.
CGS_GSS.1.4	As far as possible, backup systems should not be used during normal operation, failing which they shall be sized so as to allow for the foreseeable increase in resource requirements in the event of an incident.
CGS_GSS.2.1	If possible, redundant backup equipment shall be activated automatically.
CGS_GSS.2.2	Where a backup system is not activated automatically, the first step in handling any incident involving a service outage shall be to activate the relevant backup

	system as quickly as possible.
CGS_GMR: Management of scrapping operations	
CGS_GMR.1.1	Media containing information internal to the organisation shall be scrapped in such a way as to not be accessible to the public.
CGS_GMR.1.2	Media containing confidential information shall be scrapped in a manner that prevents access by unauthorised persons.
CGS_GDA: Authentication management	
CGS_GDA.1.1	Above a certain level of security, authentication shall be compulsory before access is granted for consultation or modification purposes.
CGS_GDA.1.2	Where applicable, the authentication operation shall involve checking the authenticated person or application's privileges.
CGS_GDA.1.3	System accesses shall be logged, if possible including at least the user's identity, the system concerned and the date and time of access.
CGS_GDA.1.4	Operations arising out of the use of access control systems shall be traced and logged in the same way as system accesses.
CGS_GDA.2.1	A person shall in all cases be authenticated on the basis of information that the person knows (password, pin code, etc.), and possibly also an object in their possession (badge, smart card, etc.), a physical attribute (biometrics) or a combination of the two.
CGS_GDA.3.1	Application authentication procedures shall be based on a system that ensures that the application cannot be usurped (e.g. signature certificate).
CGS_GDA.3.2	Certain sensitive functions (to be defined) shall automatically be subject to an authentication procedure.
CGS_CSR: Network service configuration	
CGS_CSR.1.1	All network services shall be configured so that they cannot be used for purposes other than those for which they are intended.
CGS_CSR.1.2	Connections shall be filtered to prevent unplanned traffic (asynchronous-mode operation, access via unauthorised ports, spam, etc.).
CGS_CSR.1.3	The access control system shall be capable of limiting the potential for illicit or fraudulent operations.
CGS_CME: Configuration of electronic messaging systems	
CGS_CME.1.1	E-mail and other electronic messaging systems shall be configured such that the resulting network flows can be controlled (limiting automatic message transmissions, mailing lists accessible to all users, etc.).
CGS_SUP: Supervision	
CGS_SUP.1.1	System supervision mechanisms shall be as simple and user-friendly as possible (with clear information via a single, appropriate tool allowing centralised supervision, etc.)
CGS_GDT: Trace management	
CGS_GDT.1.1	Traces shall receive at least an equivalent level of protection than the operations that they record, and possibly a greater level of protection if they contain personal data.

3.4.7 CDO : Documentation

CDO_APP: Documentation relating to applications	
CDO_APP.1.1	Application user, administration and maintenance manuals, together with any additional internal documents on the subject shall be accessible to the parties concerned.
CDO_APP.1.2	Application user, administration and maintenance procedures shall be accessible to the parties concerned.
CDO_APP.1.3	Internal documents shall be updated regularly.

CDO_SDC: Configuration monitoring	
CDO_SDC.1.1	An up-to-date inventory of systems and system configurations shall be produced, updated whenever a system or configuration is changed, and distributed to all parties that need to know such information (maintenance personnel, developers, internal support personnel, etc.)
CDO_SDC.1.2	Any changes to hardware or software configurations shall provide for compatibility with the rest of the information system and existing backups and archives. In addition, a rollback procedure shall be included as protection against any anomalies that may result from the modification.

3.4.8 CGI : Incident management

CGI_GDC: Crisis management	
CGI_GDC.1.1	Potential crisis situations shall be identified in advance.
CGI_GDC.1.2	Crisis alert thresholds shall be specified for each identified potential crisis, in order to establish when an organisation or site has entered a crisis situation.
CGI_GDC.1.3	A specific measurement shall be implemented for the purpose of detecting when alert thresholds are exceeded.
CGI_GDC.1.4	An automatic alert relay system shall be introduced, to trigger the crisis management procedure when an alert threshold is reached.
CGI_GDC.2.1	The crisis management procedure shall be triggered automatically when an alert threshold is reached.
CGI_GDC.2.2	The crisis management procedure may be triggered manually by top-tier escalated incident managers even if an alert threshold is not reached.
CGI_GDC.2.3	If no top-tier escalated incident managers are present, responsibility for manually triggering the crisis management procedure shall be transferred to someone who is present (the top-tier escalated incident manager's deputy or a specifically-identified person).
CGI_GDC.2.4	The chain for transferring responsibility for manually triggering the crisis management procedure shall be clearly identified such that somebody is always responsible even if several more senior people are unavailable.
CGI_GDC.2.5	The persons liable to manually trigger the crisis management procedure shall be made aware of and trained in the manual triggering procedure.
CGI_GDC.2.6	At its simplest, triggering the crisis management procedure shall involve promptly contacting the member in charge of the crisis unit appropriate to the situation.
CGI_GDC.3.1	Crisis units shall be formed for each type of potential crisis (physical accident, network attack, legal proceedings, etc.).
CGI_GDC.3.2	At their simplest, crisis units shall include a specialist in the relevant field of expertise and a decision-maker with the necessary authority to make decisions involving the entire organisation.
CGI_GDC.3.3	A manager and replacements shall be identified for each crisis unit.
CGI_GDC.3.4	A crisis unit's manager shall convene an immediate meeting of the unit as soon as the crisis management procedure is triggered and they are informed of the crisis.
CGI_GDC.3.5	An adequate number of replacements shall be appointed for each crisis unit member.
CGI_GDC.3.6	Crisis unit members and their replacements shall be made aware of and trained in crisis management in the relevant field.
CGI_GDC.4.1	Crisis units shall have access to all the necessary information for containing or solving a crisis.
CGI_GDC.4.2	Crisis units shall be able to make all the necessary decisions to contain or solve a crisis.
CGI_GDC.4.3	Decisions made by a crisis unit shall be implemented as quickly as possible.
CGI_GDC.4.4	All decisions made by a crisis unit shall be recorded in writing, dated and

	accompanied by the information forming the basis of the decision.
CGI_GDC.4.5	Responsibility for recording the decisions made by a crisis unit shall be assigned to somebody other than the crisis unit manager.
CGI_GDC.4.6	Decisions made by a crisis unit shall be stored, used and managed in the same way as other information system security records.
CGI_LCI: Fire-fighting	
CGI_LCI.1.1	A fire-fighting organisation shall be introduced.
CGI_LCI.1.2	The fire-fighting organisation shall comply with applicable standards.
CGI_LCI.1.3	The fire-fighting organisation shall identify appropriate fire-fighting profiles.
CGI_LCI.1.4	The role and responsibilities associated with each fire-fighting profile shall be clearly defined, in particular in terms of responsibility for evacuations.
CGI_LCI.1.5	Profiles shall be assigned to named members of the organisation.
CGI_LCI.1.6	An adequate number of replacements shall be appointed for each fire-fighting profile.
CGI_LCI.1.7	Fire-fighting profile holders and replacements shall be made aware of and trained in their roles and responsibilities.
CGI_GIS: Security incident management	
CGI_GIS.1.1	Incident management organisations shall be capable of resolving the majority of ordinary incidents in their field.
CGI_GIS.1.2	Incident management organisations shall be able to escalate any incidents that they are unable to handle to higher tiers.
CGI_GIS.1.3	Whether they handle the incident themselves or not, incident management organisations shall track incidents (incident type, date, contact person, intervention follow-up, closure date).
CGI_GIS.1.4	Any outstanding incidents shall be followed up regularly, to ensure that the search for solutions is still ongoing.
CGI_GIS.1.5	Resolved incidents shall be archived with a description of the incident's symptoms, its cause and the method used to resolve it.
CGI_GIS.1.6	The security incident handling procedure shall be regularly reviewed, to ensure that it is suited to the information system and its organisation.
CGI_GIS.1.7	The security incident handling review manager shall be clearly identified.
CGI_GIS.1.8	Any changes to the incident management procedure shall be distributed to all information system users.
CGI_GIS.2.1	The organisation responsible for managing theft-related security incidents shall conduct the formalities for declaring the theft to the police.
CGI_GIS.2.2	The organisation responsible for managing theft-related security incidents shall modify the inventory of the organisation's assets to reflect the theft.
CGI_GIS.2.3	The organisation responsible for managing theft-related security incidents shall conduct the formalities for terminating the validity of any means of authentication present on stolen equipment.
CGI_GIS.2.4	The organisation responsible for managing theft-related security incidents shall conduct any necessary administrative or legal formalities.
CGI_GIS.2.5	All theft-related security incidents shall be archived, with a record of the date, time and location of the theft, as well as a description of the circumstances.
CGI_GIS.3.1	Archived incidents shall be analysed, to assess whether coverage of the vulnerability exploited during the incident can be improved, and possibly to anticipate future incidents (e.g. system failure or saturation).
CGI_GIS.3.2	Archived incidents shall be included in a knowledge base to accelerate and simplify the resolution of similar incidents in the future.
CGI_GIS.3.3	Archived incidents shall be summarised and submitted with the results of the corresponding analysis to identified decision-makers so that they can be taken into consideration in the organisation's security strategy.

CGI_GIS.3.4	The decision-makers responsible for analysing incident summaries and their replacements shall be clearly identified.
CGI_GIS.3.5	Decision-makers responsible for analysing incident summaries and their replacements shall be made aware of and trained in this type of analysis.
CGI_GIS.3.6	Decision-makers responsible for analysing incident summaries, and where applicable their replacements, shall have the necessary authority to make decisions that could mitigate foreseeable developments.

3.4.9 CEI : Initial information system studies and design

CEI_ABS: Security sensitivities analysis	
CEI_ABS.1.1	Non-shared parts of the information system shall be secured according to the security sensitivities of the relevant functional components.
CEI_ABS.1.2	Each functional component shall be studied to ascertain its security sensitivities, in particular in terms of confidentiality, availability, integrity and control/proof.
CEI_ABS.1.3	Any specific sensitivity not covered by the information system's general security provisions shall if possible be covered by provisions specific to the functional element (technical architecture, security procedures, etc.).
CEI_ABS.1.4	A residual risk study (cf. CRR_ETU) shall be conducted for any specific sensitivity that cannot be satisfactorily covered.
CEI_ABS.1.5	The initial study shall make it possible to ascertain the necessary resources and provide a preliminary sizing approach for the system (including in peak and backup operation) and personnel (including replacements), together with the resources required for the development process.
CEI_ABS.1.6	Identified security sensitivities shall allow for any local issues and the local situation (economic, social, political and legislative context, etc.).
CEI_ABS.1.7	Identified security sensitivities shall allow for the potential impacts of incidents.
CEI_CDT: Technology choices	
CEI_CDT.1.1	Obsolescent technologies in the information system shall be replaced with sustainable technologies as quickly as possible.
CEI_CDT.1.2	Obsolescent technologies in the information system shall be replaced with sustainable technologies as quickly as possible.
CEI_CDT.2.1	Ease of use and management shall be taken into account when selecting software, hardware and facilities.
CEI_CDT.2.2	Health-related standards shall be taken into account when selecting software, hardware and facilities.
CEI_ERS: Study of specific risks relating to hardware and software	
CEI_ERS.1.1	Any specific risks relating to elements hosted by the organisation (explosive materials, flammable products, heat sources and sources of electromagnetic radiation, etc.) shall be studied and taken into account when designing and equipping sites.

3.4.10 CPS : Security policies

CPS_PPT: Workstation protection policy	
CPS_PPT.1.1	The security policy shall include a protection policy for static and mobile workstations (integrity, access control, protection against malicious software, etc.).
CPS_PPT.1.2	The workstation protection policy shall be consistent with the organisation's security sensitivities.
CPS_PPT.1.3	The workstation protection policy shall be reviewed regularly, to confirm that it is consistent with the organisation's security sensitivities.
CPS_PPT.1.4	The workstation protection policy review manager shall be clearly identified.
CPS_PPT.1.5	All workstation users shall be notified of any changes to the workstation

	protection policy.
CPS_PAQ: Quality assurance policy	
CPS_PAQ.1.1	Any operations affecting the information system shall be covered by the organisation's Quality Assurance Plan.
CPS_PAQ.1.2	The provisions of the organisation's Quality Assurance Plan shall be recorded in a Quality Assurance Manual.
CPS_PAQ.1.3	All organisation employees shall have access to the Quality Assurance Manual.
CPS_PAQ.1.4	The Quality Assurance Manual shall be reviewed regularly, to ensure that it remains consistent with the organisation's quality objectives.
CPS_PAQ.1.5	The Quality Assurance Manual review manager shall be clearly identified.
CPS_PAQ.1.6	All of the organisation's employees shall be notified of any changes to the Quality Assurance Manual.
CPS_PAQ.2.1	The Quality Assurance Manual shall cover any business-specific quality assurance considerations.
CPS_PAQ.2.2	All of the organisation's employees shall be made aware of the business-specific quality provisions, to help them comply with the quality strategy.
CPS_PAQ.3.1	Wherever possible, manual processes shall be approved by a manager before being implemented.
CPS_DEV: Software development security policy	
CPS_DEV.1.1	The development of applications for the information system shall be controlled and regulated by development rules.
CPS_DEV.1.2	CPS_DEV.1.2 Development rules shall be based on national and international development standards.

3.4.11 CPD : Data protection

CPD_DGL: Geo-location data	
CPD_DGL.1.1	Any data that can be used to physically locate a person or item of equipment shall be treated as sensitive and protected as such from a confidentiality perspective.
CPD_DGL.1.2	The organisation's personnel shall be made aware of the need to protect data that can be used to locate people or equipment.
CPD_INP: Identification of protection levels	
CPD_INP.1.1	CPD_INP.1.1 A system's protection level shall be physically marked on the system and recorded in its documentation.

3.4.12 CFO : Training

CFO_SPS: Security problem awareness	
CFO_SPS.1.1	CFO_SPS.1.1 All information system users shall be made aware of the risks to the information system, the different methods of attack, the potential security problems and the measures that can be taken to cover risks or mitigate their impact.
CFO_SPS.1.2	All personnel shall be made aware of everyday behaviour liable to impair the quality of service provided by the information system (e.g. forwarding hoaxes).
CFO_FRS: Training for replacements and successors	
CFO_FRS.1.1	CFO_FRS.1.1 An adequate number of replacements shall be identified for the organisation's important positions, in case their holders are occasionally unavailable.
CFO_FRS.1.2	Replacements assigned to fill occasionally-unstaffed positions shall be trained to perform the tasks associated with those positions.
CFO_FRS.1.3	Replacements assigned to fill occasionally-unstaffed positions shall be informed of the responsibilities relating to those positions.s à ces fonctions

CFO_FRS.1.4	Depending on the nature of the positions requiring a deputy, the deputy may be relieved of some or all of their usual duties.
CFO_FRS.1.5	While deputising for another employee, replacements shall receive all the privileges, rights, assignments and responsibilities of the person they are replacing.
CFO_FRS.2.1	Wherever possible, the departure of incumbent position holders shall be anticipated and planned for well in advance.
CFO_FRS.2.2	If, following the departure of an incumbent position holder, a team is understaffed for the duties for which it is responsible, a successor to the departing incumbent shall be identified.
CFO_FRS.2.3	A sufficiently long transitional period shall be allowed, during which the incumbent and their successor occupy the same positions.
CFO_FRS.2.4	Before leaving, departing incumbents shall train their successors and introduce them to their regular contacts.

3.4.13 CCC : Contract clauses

CCC_CLR: Contract clauses limiting the liabilities of the two parties	
CCC_CLR.1.1	The responsibilities, sanctions and penalties attributed to each party to a contract shall be appropriate to the context and consistent with the potential impacts (disproportionate penalties and sanctions should be avoided).
CCC_CLR.1.2	The liabilities of each party to a contract shall be limited by a clearly-stated maximum.
CCC_RGF: Reversibility and financial guarantees	
CCC_RGF.1.1	Measures for evaluating the financial and/or technical solidity of potential subcontractors or service providers shall be employed during the selection process.
CCC_RGF.1.2	Long-term service contracts and subcontracting agreements shall include a reversibility clause.

3.4.14 CRH : Human resources

CRH_DDE: Team sizing	
CRH_DDE.1.1	Team sizes shall be determined such that the team can perform its duties satisfactorily.
CRH_DDE.1.2	Team sizes shall be determined such that the team can perform its essential duties even when some members are unavailable.
CRH_PDP: Protection of personnel	
CRH_PDP.1.1	If the general environment is challenging, the organisation shall take measures to protect employees (protection service, accommodation near the site, etc.).
CRH_PDP.1.2	Employees working at remote sites shall have access to temporary accommodation at the main site, and be able to perform their most important tasks there.
CRH_PDP.1.3	The organisation shall develop contingency solutions for hard-to-access sites (e.g. chartering coaches to counter transport strikes, hiring snow-ploughs to clear access to the site, etc.).
CRH_CDT: Working conditions	
CRH_CDT.1.1	The workplace layout shall be well-suited to the work performed (adequate lighting, appropriate temperature, sound insulation, storage furniture, etc.).
CRH_CDT.1.2	Special measures shall be taken to minimise workplace disruption (no meetings in open-space office areas, coffee machine located away from work areas, etc.).
CRH_QDP: Employee qualifications	
CRH_QDP.1.1	The duties assigned to each employee shall correspond to their qualifications.

3.4.15 CDS : System sizing

CDS_DES: Sizing of essential services	
CDS_DES.1.1	Essential and backup services shall be sized so as to provide appropriate services and satisfactory quality of service, including during peak periods.
CDS_DES.1.2	The sizing of essential services shall be reviewed regularly and at every major change to the information system or a site, to ensure that appropriate services and satisfactory quality of service continue to be provided, including during peak periods.

4 Proposed coverage of vulnerabilities by generic security objectives

Security objectives (the codes of which correspond to those of the previous parts) are arranged by attack method and vulnerability.
The following tables are used to identify at a glance the generic security objectives liable to cover each generic vulnerability. They are therefore useful for vulnerability processing, but must nonetheless be complemented by objectives covering risk sources and consequences to ensure that the risks in question are processed thoroughly.

4.1.1 FIRE

Vulnerability	Coverage
Single copy of licence contracts	LOG_07
Single internally-developed applications	MAT_02
No substitution equipment	MAT_01
Equipment using flammable materials (e.g. bulk printers producing dust)	PHY_09
No back-up of data contained on the media	ORG_08
Original media	MAT_02 ORG_08
No insurance cover for serious damage	ORG_44
No site inspection by emergency services (fire-fighting services)	ORG_22 ORG_25
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses guaranteeing cover of the activities if a crisis is declared at the supplier's site	ORG_38
No security instructions given to external personnel working on the premises	ORG_25
No management of emergency equipment inspection reports	ORG_27
No updated display of information for calling the emergency services	ORG_17
No fire-fighting organisation (description of roles and responsibilities)	ORG_14 ORG_24
No monitoring of maintenance contracts for fire-fighting equipment	ORG_27
No crisis management organisation	ORG_14 ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No test of reaction and information procedures in the event of an accident	PER_11
No awareness programme for protection of security equipment	PER_05
Conflictual industrial relations	
Presence of an opening onto a public right-of-way (window)	PHY_03
Ageing of the premises	PHY_10
No control of access to the site or premises	PHY_03
No fire partitions	PHY_09
No precautions taken at the installation phase for fire risks specific to the equipment housed.	PHY_06
No sizing of the automatic fire extinction system, or incorrect sizing or inadequacy of this system.	PHY_09
No maintenance of air-conditioning equipment	ORG_27 PHY_01

4.1.2 WATER DAMAGE

Vulnerability	Coverage
Single copy of licence contracts	LOG_07
Single internally-developed applications	MAT_02
No substitution equipment	MAT_01
No back-up of data contained on the media	ORG_08
Original media	MAT_02 ORG_08
No insurance cover for serious damage	ORG_44
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	ORG_38
No security instructions given to external personnel working on the premises	ORG_25
No management of emergency equipment inspection reports	ORG_27
No updated display of information for calling the emergency services	ORG_17
No warning, reaction or information instructions in the event of water damage (no identification of stop cocks, etc.)	ORG_24 ORG_24
No guarantee that water detectors are operating correctly	ORG_27
No crisis management organisation	ORG_14 ORG_24
No test of reaction and information procedures in the event of an accident	PER_11
Unfamiliarity with security measures	PER_03 PER_11
No awareness programme for protection of security equipment	PER_05
Conflictual industrial relations	
Site located in flood-prone area	PHY_04
No control of physical access points to the premises	PHY_03
External opening not watertight	PHY_03
Presence of a fire extinction system using water	PHY_03
Ceiling or external opening not watertight	PHY_03
No clear identification of water stop cocks	PHY_07
Unprotected access point	PHY_03
Water pipe close to equipment	PHY_03
Fire extinction system using water	PHY_10
Water pipe close to termination equipment	PHY_03
No sump	PHY_03
Unprotected access to rooms housing production equipment or distribution equipment for essential services	PHY_03
Wiring laid on the floor	PHY_07
Ageing of cooling pipes	PHY_10
No maintenance of air-conditioning equipment	ORG_27 PHY_01
No water stop cock	PHY_07

4.1.3 POLLUTION

Vulnerability	Coverage
Single copy of licence contracts	LOG_07

Single internally-developed applications	MAT_02
Medium sensitive to storage conditions	MAT_03
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No monitoring of maintenance contracts	ORG_27
No measures in the event of interruption of air-conditioning service	ORG_16
No test of reaction and information procedures in the event of an accident	PER_11
Unfamiliarity with security measures	PER_03 PER_11
No awareness programme for protection of security equipment	PER_05
Conflictual industrial relations	
Proximity of pollution sources (noise, smoke, vapour, etc.)	PHY_04
Polluted atmosphere (hangar, workshop, etc.)	PHY_04
No maintenance of air-conditioning equipment	ORG_27 PHY_01
No correctly sized redundant equipment	PHY_01
Ageing of air-conditioning filters	PHY_10
Unprotected access to equipment	PHY_03

4.1.4 MAJOR ACCIDENT

Vulnerability	Coverage
Single copy of licence contracts	LOG_07
Single internally-developed applications	MAT_02
No substitution equipment	MAT_01
No back-up of data contained on the media	ORG_08
Original media	MAT_02 ORG_08
No emergency service close to the organisation	ORG_24
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
No updated display of information for calling the emergency services	ORG_17
No insurance cover for serious damage	ORG_44
No crisis management organisation	ORG_14 ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No emergency situation management procedures	PER_11
Possibilities of destruction caused by an external event (collisions, attacks)	PHY_04
Proximity of industrial activity or potentially hazardous site	PHY_04
Rooms in which explosion/implosion risks have not been taken into account	PHY_03

4.1.5 DESTRUCTION OF EQUIPMENT OR MEDIA

Vulnerability	Coverage
Single copy of licence contracts	LOG_07
Single internally-developed applications	MAT_02
No substitution equipment	MAT_01

Fragility of equipment	ORG_04
Equipment accessible to persons other than its owners (e.g. located in a passage way)	PHY_03
Medium accessible to persons other than its owners	PHY_03
No archiving procedure	ORG_07
Fragility of media	ORG_04
No archive storage measures suitable for the storage periods (ageing of tapes, wear of CD-ROMs)	MAT_04
No back-up of data contained on the media	ORG_08
Original media	MAT_02 ORG_08
No instructions given to external personnel working on the premises	ORG_25
No insurance cover for destruction of equipment	ORG_44
No rules for the use and storage of hardware and information media (protection conditions during transport, smoking ban, etc.)	ORG_04
Unfamiliarity with security measures	PER_03 PER_11
Conflictual industrial relations	
Inadequate awareness programme concerning physical protection of equipment	PER_01 PER_03
No control of access to the site or premises or possibility of intrusion via indirect access routes.	PHY_03
Unprotected physical access to rooms housing equipment or media.	PHY_03
Media accessible to unauthorised persons	ORG_01
Unidentified underground equipment	PHY_03
Equipment accessible to unauthorised persons	ORG_01
Fragility of equipment	ORG_04

4.1.6 CLIMATIC PHENOMENON

Vulnerability	Coverage
Conditions of use outside operating limits of the equipment	PHY_01
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No emergency service close to the organisation	ORG_24
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
No instructions (warning, prevention, reaction, etc.)	ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No test of reaction and information procedures in the event of an accident	PER_11
No means of ventilation or air-conditioning during excessive summer heat	PHY_01
Climatic conditions not taken into account in the construction of the premises	PHY_04
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	MAT_03

4.1.7 SEISMIC PHENOMENON

Vulnerability	Coverage
Equipment sensitive to vibrations	PHY_03
No installation standard for sites belonging to the organisation	ORG_23 ORG_38

No emergency service close to the organisation	ORG_24
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
No instructions (warning, prevention, reaction, etc.)	ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No test of reaction and information procedures in the event of an accident	PER_11
Seismic conditions not taken into account in the construction of the buildings	PHY_04
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	MAT_03

4.1.8 VOLCANIC PHENOMENON

Vulnerability	Coverage
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No emergency service close to the organisation	ORG_24
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
No instructions (warning, prevention, reaction, etc.)	ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No test of reaction and information procedures in the event of an accident	PER_11
Site listed as volcano-prone	PHY_04
Seismic conditions not taken into account in the construction of the buildings	PHY_04
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	MAT_03

4.1.9 METEOROLOGICAL PHENOMENON

Vulnerability	Coverage
Conditions of use outside operating limits of the equipment	PHY_01
No emergency service close to the organisation	ORG_24
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
No instructions (warning, prevention, reaction, etc.)	ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No test of reaction and information procedures in the event of an accident	PER_11
Site in which extreme weather phenomena occur periodically (storm, hurricane, cyclone, etc.)	PHY_04
No protection against lightning	PHY_04
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	MAT_03

4.1.10 FLOOD

Vulnerability	Coverage
No emergency service close to the organisation	ORG_24

No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
No instructions (warning, prevention, reaction, etc.)	ORG_24
Site located in flood-prone area	PHY_04
No protection against rising water levels	PHY_03
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	MAT_03

4.1.11 FAILURE OF AIR-CONDITIONING

Vulnerability	Coverage
Equipment requiring air-conditioning in order to operate	MAT_03 PHY_01
Archives requiring air-conditioning for their preservation	MAT_03 PHY_01
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses covering compensation for damage in the event of loss of an essential service	ORG_38
No contractual clauses covering the maximum acceptable downtime of an essential service	ORG_38
No instructions (warning, prevention, reaction, etc.)	ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No revision of air-conditioning needs when premises are modified or equipment is added.	PHY_01
System depending on a chilled water or power supplier	PHY_01
System not adequately sized to meet the needs	PHY_01
No maintenance of air-conditioning equipment	ORG_27 PHY_01
No correctly sized redundant equipment	PHY_01
Unprotected access to water and power supply equipment	PHY_03

4.1.12 LOSS OF POWER SUPPLY

Vulnerability	Coverage
Equipment sensitive to electrical disturbances (voltage drops, overvoltages, transient power-cuts)	PHY_01
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses covering compensation for damage in the event of loss of an essential service	ORG_38
No contractual clauses covering the maximum acceptable downtime of an essential service	ORG_38
No instructions (warning, prevention, reaction, etc.)	ORG_24
Unfamiliarity with security measures	PER_03 PER_11
Lack of information concerning conditions of use of emergency power supply points	PER_11
Terminal communication equipment with no emergency power supply	PHY_01

Rooms containing acid-based batteries are not specifically designed and physically isolated from the equipment to which they are connected	PHY_06
Incorrect sizing of emergency power supply equipment (inverter, batteries, etc.)	PHY_01
Unprotected physical access to rooms housing electrical power supply and distribution equipment	PHY_03
Rooms containing acid-based batteries are not fitted with mechanical ventilation and explosion-proof electrical equipment.	PHY_06
The floor or wall coverings are not anti-static	PHY_03
The low voltage panel is not accessible	PHY_01
The medium / low voltage transformer substation is not installed on the site (with controlled supplier access)	PHY_01
No analysis of emergency power level required if equipment is added	PHY_01
Earthing of exposed conductive parts does not comply with regulations	PHY_10

4.1.13 FAILURE OF TELECOMMUNICATION EQUIPMENT

Vulnerability	Coverage
Equipment maintained remotely via telecommunication equipment	PHY_01
No installation standard for sites belonging to the organisation	ORG_23 ORG_38
No contractual clauses covering compensation for damage in the event of loss of an essential service	ORG_38
No contractual clauses covering the maximum acceptable downtime of an essential service	ORG_38
No instructions (warning, prevention, reaction, etc.)	ORG_24
Unfamiliarity with security measures	PER_03 PER_11
No maintenance of termination and distribution equipment	PHY_01
Operating faults on the internal telephone network	PHY_01
Operating problem already encountered on the telecommunication service supply	PHY_01
Unprotected physical access to rooms housing electrical power supply and distribution equipment or telecommunication equipment	PHY_03

4.1.14 ELECTROMAGNETIC RADIATION

Vulnerability	Coverage
Equipment or medium sensitive to electromagnetic or thermal radiation	PHY_03
No contractual clause relating to electromagnetic compatibility	ORG_38
Risk of electromagnetic or thermal radiation not taken into account in the design	PHY_03
Proximity of a source of electromagnetic or thermal radiation	PHY_03
Risks arising from the proximity of an electromagnetic source not taken into account	PHY_03
Medium and supports sensitive to electromagnetic or thermal radiation	PHY_10

4.1.15 THERMAL RADIATION

Vulnerability	Coverage
Equipment or medium sensitive to electromagnetic or thermal radiation	PHY_03
Proximity of a source of electromagnetic or thermal radiation	PHY_03
Risk of electromagnetic or thermal radiation not taken into account in the design	PHY_03

Risks arising from the proximity of an electromagnetic source not taken into account	PHY_03
Medium and supports sensitive to electromagnetic or thermal radiation	PHY_10

4.1.16 ELECTROMAGNETIC PULSES

Vulnerability	Coverage
Equipment or medium sensitive to electromagnetic or thermal radiation	PHY_03
Proximity of a source of electromagnetic or thermal radiation	PHY_03
Risk of electromagnetic or thermal radiation not taken into account in the design	PHY_03
Risks arising from the proximity of an electromagnetic source not taken into account	PHY_03
Medium and supports sensitive to electromagnetic or thermal radiation	PHY_10

4.1.17 INTERCEPTION OF COMPROMISING INTERFERENCE SIGNALS

Vulnerability	Coverage
Installation rules not taken into account	MAT_14 PHY_10
Equipment zoning not taken into account	PHY_03
Equipment capable of emitting compromising stray radiation	PHY_05
Managers have no contact with the expertise or technology watch departments	ORG_34
No rules imposing the use of standards	ORG_04
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	ORG_38
No equipment verification procedure before purchase or after maintenance work.	ORG_20
No monitoring of security policy application	ORG_22
No information protection policy	ORG_15
The security policy is not applied	ORG_18
TEMPEST zoning not carried out	PHY_05
Public access close to the buildings	PHY_05
Room situated close to a public right-of-way	PHY_05
Ancillary equipment making it easier to pick up compromising stray signals (electrical cables, pipes, etc.)	PHY_05
No protection of access to equipment	PHY_03
Medium and supports capable of emitting compromising stray radiation	PHY_05

4.1.18 REMOTE SPYING

Vulnerability	Coverage
No screen saver when equipment is inactive	LOG_16
Use of easily-observed passwords to access the system or application (shape on keyboard, short password)	ORG_10
Password for accessing the system or application changed rarely or not at all	ORG_10
Screen observable from outside	PHY_02
Sensitive documents read in public places (documents observed by external persons, etc.)	ORG_15
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_02 ORG_04 ORG_27 ORG_30

	ORG_33 ORG_38
No rules for protecting the exchange of confidential information	ORG_15
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	ORG_38
The security policy is not applied	ORG_18
No identification of sensitive assets	ORG_26
The security responsibilities concerning authorisation management are not formalised.	ORG_14 ORG_15
No monitoring of application of the security policy	ORG_22
No information protection policy	ORG_15
No identification of security needs for a project	ORG_32
Unfamiliarity with security measures	PER_03 PER_11
Low awareness of the need to protect information	PER_02
No management support for application of the security policy	PER_13
Presence of observation point outside the site	PHY_02
Zone with opening onto a public right-of-way	PHY_02
Zone observable from a passage way	PHY_07

4.1.19 EAVESDROPPING

Vulnerability	Coverage
No access monitoring device when equipment is inactive	LOG_13
Possibility of adding an eavesdropping programme such as a Trojan horse	LOG_08
No protection of logs containing activity tracks	ORG_15 ORG_39
Password for accessing the system or application changed rarely or not at all	ORG_10
No protection against the use of advanced privileges	LOG_11
Password for accessing support software changed rarely or not at all	ORG_10
Logical access to equipment allowing eavesdropping software to be installed	MAT_10
Equipment with a communication interface that can be eavesdropped (infrared, 802.11, Bluetooth, etc.)	RES_02
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
No rules for protecting the exchange of confidential information	ORG_15
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	ORG_38
No monitoring of application of the security policy	ORG_22
No identification of sensitive assets	ORG_26
The security responsibilities concerning authorisation management are not formalised.	ORG_14 ORG_15
The security policy is not applied	ORG_18
No information protection policy	ORG_15
No identification of security needs for a project	ORG_32
Insufficient training in measures and tools for protecting external and internal	PER_03

exchanges	
Personnel susceptible to enticement	PER_02
No management support for application of the security policy	PER_13
Low awareness of the need to protect the confidentiality of information exchanges	PER_09
Obtaining an advantage through picking up information	PER_08
Possibility of picking up transmissions outside the site	PHY_05
No control of access to the site or premises or possibility of intrusion via indirect access routes.	PHY_03
Access to communication terminal equipment not protected	RES_01
Medium and supports whose characteristics allow eavesdropping (e.g. Ethernet, wireless communication systems)	RES_02
Physical or logical access to a relay allowing eavesdropping equipment to be installed	ORG_01
No authentication of equipment connected to the network	RES_03
Physical access to communication support or equipment allowing eavesdropping equipment to be installed	PHY_03 RES_01
Communication in broadcast mode	RES_02
Complex routing between sub-networks	RES_05
Interface with a function that allows eavesdropping	RES_01 RES_02
Circulating information in clear text	RES_02
No partitioning of communication networks	RES_02
Possibility of eavesdropping on exchanges with authentication servers	RES_02
Possibility of eavesdropping on exchanges with application servers	RES_02
Possibility of introducing eavesdropping software on client terminals	LOG_08
Possibility of installing an eavesdropping device on messaging gateways	LOG_08
Flaws in the management of access privileges to messaging gateways	LOG_11

4.1.20 THEFT OF MEDIA OR DOCUMENTS

Vulnerability	Coverage
Single internally-developed applications	MAT_02
No equipment inventory	MAT_06
Tempting equipment (trading value, technology, strategic)	MAT_07
No protection of equipment against theft (anti-theft cable)	MAT_07
Easily removed hard disc	MAT_07
Equipment used on self-service basis by a number of persons	MAT_07
Access to back-up equipment not protected	MAT_07
Printer present in passage way	ORG_01 PER_02
Media available to everyone	MAT_07 ORG_15 ORG_30
Media sent via postal services (external service providers, internal mail service, etc.)	ORG_03
Media storage not protected	MAT_07
No inventory of media used	MAT_06
No back-up of data contained on the media	ORG_08

Easily transported media (e.g. removable hard disc, back-up cartridge)	MAT_07
Original media	MAT_02 ORG_08
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_15 ORG_38
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	ORG_38
Security responsibilities concerning the classification of information are not formalised or known by everyone	ORG_14 ORG_15
The security policy is not applied	ORG_18
No organisation for management of security incidents	ORG_21
No identification of sensitive assets	ORG_26
No monitoring of sensitive assets	ORG_04 ORG_15
No monitoring of application of the security policy	ORG_22
No identification of security needs for a project	ORG_32
No information protection policy	ORG_15
Personnel susceptible to enticement	PER_02
Failure to follow rules concerning information classification.	PER_03
Low awareness of the need to protect confidential documents, leading to a lack of vigilance	PER_02
Obtaining an advantage through disclosing information	PER_08
No management support for application of the security policy	PER_13
No individual commitment to protect confidential documents	PER_05
Media or documents sent or present outside the site	PER_01
No control of access to the site or premises or possibility of intrusion via indirect access routes.	PHY_03

4.1.21 THEFT OF EQUIPMENT

Vulnerability	Coverage
No substitution equipment	MAT_01
No equipment inventory	MAT_06
Equipment freely available to a number of persons	MAT_07
Tempting equipment (trading value, technology, strategic)	MAT_07
Equipment that can be resold (no marking, used without password)	MAT_07
Easily dismantled equipment	MAT_07
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	ORG_38
No organisation for management and treatment of security incidents linked to theft	ORG_21
No monitoring of application of the security policy	ORG_22
No rules for checking equipment entering/leaving the organisation	ORG_02
No identification of sensitive assets	ORG_26
No identification of security needs for a project	ORG_32

No management support for application of the security policy	PER_13
Low awareness of the need to protect equipment outside the organisation	PER_01
Personnel susceptible to enticement	PER_02
Failure to follow the rules concerning physical protection of transportable equipment	PER_01 PER_08
Obtaining an advantage through selling equipment	PER_08
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	PER_01
No control of access to the site or premises or possibility of intrusion via indirect access routes.	PHY_03

4.1.22 RETRIEVAL OF RECYCLED OR DISCARDED MEDIA

Vulnerability	Coverage
Presence of residual data used by the software	MAT_08
Presence of residual data unknown to the user of reallocated or discarded equipment	MAT_08
No means of destroying the media	MAT_08
No identification of sensitive assets	ORG_26
No monitoring of sensitive assets	ORG_04 ORG_15
No monitoring of application of the security policy	ORG_22
No information protection policy applicable to recycling and discarding	ORG_15
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	ORG_38
Personnel susceptible to enticement	PER_02
Failure to comply with rules concerning the destruction of media containing classified information	PER_02
No information or awareness concerning residual data on media	PER_02
Obtaining an advantage through disclosing information	PER_08
No management support for application of the security policy	PER_13
Presence of discarded media outside the site	ORG_15
Presence of discarded media in public places	ORG_15
Presence of discarded media in zones accessible to persons who have no need to know	ORG_15

4.1.23 DISCLOSURE

Vulnerability	Coverage
No verification of approved shared access	LOG_13 MAT_10
Procedures for managing access privileges too heavy to operate	ORG_36
Access right management functions too complicated to use and capable of producing an error	MAT_11
Presence of shared directory for storing information	MAT_10
Media can be used to exchange sensitive information	MAT_10
No structure responsible for defining, implementing and monitoring access privileges to information	ORG_14 ORG_30
No identification of sensitive assets	ORG_26
The security policy is not applied	ORG_18

No personal commitment to protect confidentiality	ORG_37 PER_05
Procedures for managing and applying authorisation too heavy to use	ORG_36
Security responsibilities concerning the classification of information are not formalised or known by everyone	ORG_14 ORG_15
No monitoring of sensitive assets	ORG_04 ORG_15
No information protection policy	ORG_15
Failure to observe information classification rules	PER_03
No management support for application of the security policy	PER_13
Personnel susceptible to enticement	PER_02
Inadequate awareness of the need to protect sensitive information	PER_03
Failure to observe discretion	PER_09
Obtaining an advantage through disclosing information	PER_08
No checking (or tracking) of exchanges with the outside	PHY_07
Presence of a communication network with the outside allowing exchange of information	RES_02
Complex or unpractical files	ORG_42
Standard interface allowing information exchanges (e.g. Bluetooth interface accepting all communications by default)	RES_02
Resources can be used without tracking	RES_03
No user notification	RES_03
Complex routing between sub-networks	RES_05
No strict routing between sub-networks	RES_05
No filtering and logging on communication relays between networks	RES_02 RES_03
The system is connected to external networks	RES_02
No control of access to information stored in the directory	LOG_11
No access logging	RES_03
No filtering system	RES_02
Access privileges to shared information difficult to manage or not managed at all (definition, implementation, monitoring)	LOG_11
No partitioning of communication networks	RES_02
No measure to avoid negligence when information is sent	LOG_17
The system can be used by all personnel	LOG_13
The system allows attachments to be exchanged	PER_02
No effective and operational virus shield	ORG_06
No management of information access privileges (possibility of corrupting public data, etc.)	LOG_11
The system makes it easy to disclose information to the outside	PER_02

4.1.24 DATA FROM UNTRUSTWORTHY SOURCES

Vulnerability	Coverage
Software retrieval from a non-authenticated source	LOG_06 LOG_08
Possibility of installing correction programmes, updates, patches, hotfixes, etc.	LOG_08 LOG_11 LOG_03

No sure means of identification	LOG_13
No storage of activity tracks	LOG_10
No means of guaranteeing the source of equipment	ORG_20
Managers have no contact with the expertise or technology watch departments	ORG_34
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_15 ORG_38
No means of guaranteeing the source of supplies	ORG_20
No monitoring of application of the security policy	ORG_22
No policy for storing and analysing activity tracks	ORG_39
No information concerning the division of responsibility and means of guaranteeing the legitimacy of a request.	ORG_14
No structure allowing identification of a person to be guaranteed within the organisation or a project	ORG_33
No management support for application of the security policy	PER_13
No awareness programme concerning the risks of usurping of identity (misuse of means of authentication such as passwords)	PER_03
Credulity	PER_02
Failure to appreciate the importance of qualifying information	PER_10
Personnel susceptible to enticement	PER_02
Conflictual industrial relations	
Obtaining an advantage through misinforming	PER_08
No means of guaranteeing the authenticity of codes	ORG_20
Unfamiliarity with security measures	PER_03 PER_11
Possibility of corrupting a communication	RES_02
Protocol not allowing safe authentication of the sender of a communication	RES_03
Resources can be used without tracking	RES_03
Assignment files too complex or unpractical	ORG_42
The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)	RES_03
Possibility of usurping the directory function	RES_01
The system does not allow the author of a modification to be identified	LOG_10
The system allows access to data that cannot be authenticated (e.g. hoax)	ORG_12
The system does has no means of preserving the activity history	RES_03
The system allows information to be stored or modified without authentication of the authors	RES_03
The system allows information to be sent and received without authentication of the senders or recipients	RES_03
The system has no filter to prevent hoaxes being received from the outside	ORG_12
The system allows relaying	RES_01
The system does not allow the person issuing a request to be identified	RES_03

4.1.25 TAMPERING WITH HARDWARE

Vulnerability	Coverage
Additional hardware items can be fitted for storing, transmitting or corrupting information (e.g. physical keylogger).	MAT_10 RES_01
No procedure for checking work carried out by external personnel on the organisation's equipment	ORG_25

No monitoring of application of the security policy	ORG_22
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Managers have no contact with the expertise or technology watch departments	ORG_34
No operational qualification procedures	ORG_26
No monitoring of sensitive assets	ORG_04 ORG_15
No identification of sensitive assets	ORG_26
No procedures for validating hardware components when they are delivered or returned from maintenance	ORG_20
Software not adequately tested before acceptance, especially concerning limit values	ORG_26
Personnel susceptible to enticement	PER_02
No vigilance when a maintenance agent works on a workstation or server	PER_05
Low awareness of the need to protect equipment outside the organisation	PER_01
Obtaining an advantage through misinforming	PER_08
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	PER_01
No control of access to the site or premises or possibility of intrusion via indirect access routes.	PHY_03
Possibility of circuit derivation	RES_01

4.1.26 TAMPERING WITH SOFTWARE

Vulnerability	Coverage
The remote maintenance link is permanently activated	LOG_12 RES_06
Possible existence of hidden functions introduced during the design and development phase	ORG_20 ORG_38
Possibility of modifying or corrupting the software	LOG_01
No protection against the use of advanced privileges	LOG_11
Use of non-evaluated software	LOG_06
No implementation of basic security rules applicable to the operating system and software	LOG_04
Possibility of creating or modifying system commands	LOG_08 LOG_11
Software retrieval from a non-authenticated source	LOG_06 LOG_08
Possibility of remote administration of the system using non-encrypted administration tools	RES_02
Connection passwords not sufficiently complex	ORG_10
Possibility of installing correction programmes, updates, patches, hotfixes, etc.	LOG_08 LOG_11 LOG_03
Possibility of remote system administration	RES_01 RES_06
Use of a standard operating system on which logical attacks have already been carried out	LOG_06

Possibility of remote system administration from any station	LOG_11
Possibility of deleting, modifying or installing new programmes	LOG_08
The SNMP layer is activated	LOG_12 RES_06
The equipment can be booted from any peripheral (e.g. floppy disc, CD-ROM)	MAT_10
No means of checking the safety of media when they enter the organisation	ORG_06
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Managers have no contact with the expertise or technology watch departments	ORG_34
No procedure for checking work carried out by external personnel on the organisation's equipment	ORG_25
No contractual clauses guaranteeing the safety of supplies delivered by a subcontractor or supplier	ORG_20 ORG_38
No global policy for fighting against malicious code	ORG_06
No identification of sensitive assets	ORG_26
No monitoring of application of the security policy	ORG_22
No monitoring of sensitive assets	ORG_04 ORG_15
No policy for protecting the workstations	ORG_04 ORG_06
No policy for storing and analysing activity tracks	ORG_39
No measures for checking developments	ORG_20
No measures for protecting code integrity during the design, installation and operation phases	ORG_04 ORG_20
Use of software without a guarantee of its source	PER_10
Conflictual industrial relations	
Low awareness of the threat posed by malicious codes	PER_03
Correct reflex actions not known if an anomaly is detected	PER_11
Failure to comply with anti-virus software updating rules	PER_03
Personnel susceptible to enticement	PER_02
Obtaining an advantage through disrupting the information system	PER_08
Conflictual situation	
Unfamiliarity with security measures	PER_03 PER_11
No means of guaranteeing the authenticity of developments	ORG_20
Operator or maintainer with extended privileges	PER_02
Unfamiliarity with emergency procedures if an anomaly is detected	PER_03
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	PER_01
No control of access to the site or premises or possibility of intrusion via indirect access routes.	PHY_03
The network makes it easy for unauthorised persons to use the resources	RES_01
Assignment files too complex or unpractical	ORG_42
Possibility of adding software derivations	RES_01
The network allows the system resources to be modified or adjusted	RES_01

Additional software can be added for storing, transmitting or corrupting information (e.g. keylogger)	RES_01
Resources can be used without tracking	RES_03
Applications can be modified or changed	LOG_11
Programmes or system files can be deleted or modified	LOG_11
No awareness programme concerning risks incurred through downloading software	PER_03
No anti-virus check on exchanges	ORG_06
The system allows asynchronous operation of certain parts or commands of the operating system (e.g. JavaScript components exploring the hard disc content)	LOG_04 LOG_11
Presence of a device allowing remote modification or installation of applications	LOG_11
Use of shared storage space	LOG_11
Use of an obsolete version of the messaging server	LOG_09 ORG_13
Use of a distribution list that includes a large part of the personnel	ORG_12
Presence of protocol that has no authentication function	RES_03
The messaging system allows automatic message transmission	LOG_14 ORG_06
No awareness programme concerning the risks incurred by opening attachments	PER_03
The system allows asynchronous operation of certain parts or commands of the operating system to be exploited (e.g. automatic opening of attachments)	LOG_04
Applications are not checked before installation	LOG_06
The messaging system allows software updates to be installed (e.g. patches, anti-virus updates, etc.)	LOG_11
No anti-virus filtering system	ORG_06
Pirated programmes can be installed	LOG_11

4.1.27 POSITION DETECTION

Vulnerability	Coverage
Locatable equipment (e.g. triangulation)	PHY_05
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_15 ORG_38
No rules for protecting the confidentiality of information that can be used to locate a personnel member (ticket requests, entry/exit records, etc.)	ORG_15
Unfamiliarity with security measures	PER_03 PER_11
Lack of discretion or vigilance	PER_09
No management support for application of the security policy	PER_13

4.1.28 EQUIPMENT FAILURE

Vulnerability	Coverage
No diagnostic function to prevent equipment failures	LOG_14
No protection against electrical disturbances	PHY_03
Incorrect operating conditions	MAT_14
Maintenance fault	ORG_27
Poor equipment reliability	MAT_15
Ageing of the equipment	ORG_13
Medium unsuitable for the life of data to be stored	MAT_03

	MAT_04
Poor storage conditions	PHY_03
No clause covering response time for repair and replacement in the event of equipment failure	ORG_38
Maintenance contract monitoring not organised	ORG_27
No monitoring of maintenance and support contracts with suppliers	ORG_27
No failure reporting (volumes, cost of incidents, downtime)	ORG_21
No rules covering conditions of use of information processing infrastructures (ban on smoking, drinks and food in rooms housing IT equipment)	ORG_04 PHY_08
No continuity plan covering the organisation's essential activities	ORG_16
No quick response instructions to protect equipment in the event of water damage or fire	ORG_24
Analysis of match between needs and equipment capabilities not organised	ORG_09
No rules covering conditions of use of information processing infrastructures (ban on smoking, drinks and food in rooms housing IT equipment)	
No implementation of incident monitoring to foresee failures or saturation (trend charts)	PER_05
No passing up of information for a centralised failure analysis	PER_05
Unfamiliarity with the instructions for using the equipment	PER_03
Failure to take into account a specific environment that increases the risks of failure (overheated atmosphere, industrial environment, etc.)	PHY_10
No checking to confirm that emergency resources operate correctly	ORG_16
Manual triggering of the emergency solution	ORG_16
Poor medium reliability	MAT_15
Ageing of the medium	ORG_13

4.1.29 EQUIPMENT MALFUNCTION

Vulnerability	Coverage
No diagnostic function to prevent equipment failures	LOG_14
No protection against electrical disturbances	PHY_03
Incorrect operating conditions	MAT_14
Poor equipment reliability	MAT_15
Possibility of incompatibility between equipment items	RES_04
Medium unsuitable for the life of data to be stored	MAT_03 MAT_04
Poor storage conditions	PHY_03
No incident monitoring to foresee failures or saturation (trend charts)	ORG_09
No rules imposing the use of standards	ORG_04
No clause covering response time for repair and treatment in the event of malfunction	ORG_38
No reporting on malfunctions	ORG_21
No continuity plan covering the organisation's essential activities	ORG_16
No operational qualification procedures	ORG_26
No rules covering the operating environment of information processing infrastructures (temperature, humidity, etc.)	ORG_04 PHY_10
Analysis of match between needs and equipment capabilities not organised	ORG_09
No implementation of incident monitoring to foresee failures or saturation (trend charts)	PER_05

Unfamiliarity with the instructions for using the equipment	PER_03
No passing up of information for a centralised failure analysis	PER_05
Failure to take into account a specific environment that increases the risks of failure (overheated atmosphere, industrial environment, etc.)	PHY_10
No checking to confirm that emergency resources operate correctly	ORG_16
Manual triggering of the emergency solution	ORG_16
Ageing of the medium	ORG_13
Possibility of incompatibility between the media and other components	RES_04
Medium and supports with technical characteristics specific to their locality (e.g. different ADSL configuration parameters between France and the United Kingdom)	RES_04
Poor medium reliability	MAT_15
Maintenance fault	ORG_27
Interface with technical characteristics specific to the country (e.g. different telephone connectors between France and the United Kingdom)	RES_04
Possibility of incorrect configuration, installation or modification of relays	RES_04
Ageing of the equipment	ORG_13
Possibility of incompatibility between resources	RES_04

4.1.30 SATURATION OF THE INFORMATION SYSTEM

Vulnerability	Coverage
No filter to protect the system against saturation	LOG_14
Unnecessary use of resources	LOG_14
Application requiring computing resources not matched by the equipment (e.g. insufficient RAM)	MAT_09
Requirements defined for a project without taking into account special situations that put the system under limit conditions.	LOG_14
No qualification of developments in a context representative of operation	LOG_06
Incorrect sizing of resources (e.g. insufficient reserve time on a laptop battery).	MAT_09
Unwanted persistence of data on media	ORG_09
No rules imposing the use of standards	ORG_04
No incident monitoring to foresee failures or saturation (trend charts)	ORG_09
No contractual clause covering the quality of service of systems placed under limit conditions (intense demand on the system, input of non-compliant data, input of data corresponding to operating limits)	ORG_38
No policy for checking the correct sizing of the equipment of the information processing infrastructure, including the emergency equipment	ORG_09
No instructions for avoiding the use of IT resources in a manner that leads to saturation of storage spaces or processing resources.	ORG_09
No instructions relating to incidents (detection, action, etc.)	ORG_24
No decision to resize when significant increases in the use of IT resources are observed.	PER_05
No implementation of incident monitoring to foresee failures or saturation (trend charts)	PER_05
Insufficient training in the correct use of the information tool (disturbance of the system, installation of incompatible software, etc.)	PER_03 PER_12
Obtaining an advantage through disrupting the information system	PER_08
Low awareness of the need to economise the organisation's IT resources (poor use of storage spaces, etc.)	PER_03

Incorrect sizing of telecommunication resources, resulting, for example, from daily use of resources intended for the emergency solution.	ORG_16
Incorrect sizing of emergency resources	ORG_16
Possibility of subjecting the relays to an excessive number of requests or intense interference (e.g. denial of service attacks such as smurfing, SYN flood etc.)	LOG_14 MAT_05
Possibility of incorrect configuration, installation or modification of relays	RES_04
Incorrect sizing (e.g. too much data for the maximum passband)	RES_02
Incorrect sizing of resources (e.g. too many users for the maximum capacity of the directory)	ORG_09
Possibility of subjecting the system to an unlimited number of requests	ORG_09
Existence of periods or events that cause a very significant increase in use of the system	ORG_09
Incorrect sizing of resources (e.g. too many users for the number of connections possible and the passband)	ORG_09
No management of write rights in shared storage spaces.	LOG_11
Incorrect sizing of resources (e.g. not enough storage or file share space)	ORG_09
No partitioning of communication networks	RES_02
Use of the internal distribution list accessible to everyone	ORG_12
Incorrect sizing of storage spaces for received messages	ORG_09
The messaging system allows automatic message transmission	LOG_14 ORG_06
No protection against spam	ORG_12
No limits on the size of attachments	LOG_14
Incorrect use of the messaging service (mailboxes used as storage space)	PER_03
Public access to the gateway	ORG_09
Incorrect sizing of resources (e.g. too many simultaneous connections)	ORG_09

4.1.31 SOFTWARE MALFUNCTION

Vulnerability	Coverage
Possible side effects after updating a software component	LOG_02
No storage of processing tracks	LOG_10
Lack of training in maintaining and operating new equipment	ORG_14 PER_06 PER_12
No maintenance procedure	LOG_09 ORG_41
No systematic qualification procedure before installation or updating	LOG_06
No clock synchronisation procedure	LOG_10
No passing up of information for a centralised malfunction analysis	LOG_15
Possibility of incorrect configuration, installation or modification of the operating system	LOG_04
No report for maintenance operations	LOG_08 LOG_03
Configuration of software components not managed or prone to management errors (e.g. application of a UK patch not adapted to a FR version)	LOG_08
Documentation not up to date	ORG_28
Applications are not checked before installation	LOG_06
Use of an obsolete version of the operating system or applications	LOG_09 ORG_13

No rules imposing the use of standards	ORG_04
No incident monitoring to foresee failures or saturation (trend charts)	ORG_09
No contractual clauses covering support and call-out conditions	ORG_38
No policy for partitioning user environments to avoid unintentional assignment of rights to modify the system and application	ORG_33
No instructions aimed at eliminating risk-inducing behaviour in the use of information resources	ORG_04
No instructions relating to incidents (detection, action, etc.)	ORG_24
No continuity plan covering the organisation's essential activities	ORG_16
The computing equipment is not homogenous	ORG_42
Software not adequately tested before acceptance (test data set does not cover all the operating conditions - intense demand on the system, input of non-conforming data, input of data corresponding to operating limits)	ORG_26
No incident monitoring to foresee malfunctions (trend charts)	PER_05
Lack of training	PER_12
No security rules for developments	PER_10
No training in the use and maintenance of new software	PER_12
Incorrect sizing of operating and maintenance resources	ORG_09
Failure to follow work procedures	PER_03
Insufficient training in the correct use of the information tool (disturbance of the system, installation of incompatible software, etc.)	PER_03 PER_12
Possibility of incorrect configuration, installation or modification of relays	RES_04
Poor management of pilot releases and configurations	RES_04
Interface side effects (compatibility problems between protocols, etc.)	RES_04
Possibility of the system being subjected to badly formed requests and data (e.g. buffer overflow, denial of service on LDAP server)	LOG_14
Failure to comply with installation or maintenance procedures.	ORG_04
Possibility of subjecting the system to an unlimited number of requests	ORG_09
Software incompatibility (e.g. side effect of message-filtering anti-virus software, etc.)	RES_04
Possibility of the system being subjected to badly formed requests and data (e.g. buffer overflow, denial of service on SMTP, POP3, IMAP server)	LOG_14
Use of an obsolete version of the messaging server	LOG_09 ORG_13

4.1.32 BREACH OF INFORMATION SYSTEM MAINTAINABILITY

Vulnerability	Coverage
Applications are not checked before installation	LOG_06
No emergency procedure	ORG_24
No backtrack procedure in the event of a modification error	LOG_02
No maintenance procedure	LOG_09 ORG_41
Documentation not up to date	ORG_28
No report of maintenance operations	LOG_08 LOG_03
No storage of processing and modification tracks	LOG_03
Specific software	ORG_09
No training in the use and maintenance of new software	ORG_14

	PER_06 PER_12
Obsolete software	LOG_09
Non-upgradable software	LOG_06
Inaccessibility of support media outside the organisation or from a country with a large time difference	MAT_13
Non-upgradable hardware	ORG_13
Obsolete hardware	ORG_13
Specific hardware	ORG_09 ORG_27
Back-up hardware, software or procedures modified without taking old back-ups or archives into account	ORG_05
Obsolete medium	ORG_13
Loss or poor management of original documents (support contracts, licences, etc.)	ORG_08
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
No contractual clause covering the activity (in the event of shutting down the activity, supplier bankruptcy, etc.)	ORG_38
No guarantee of the organisation's durability	ORG_27
No monitoring of maintenance and support contracts with suppliers	ORG_27
No instructions relating to incidents (detection, action, etc.)	ORG_24
No Quality Assurance Manual	ORG_29
No organisation for protecting documentation and system maintenance resources	ORG_30
No continuity plan covering the organisation's essential activities	ORG_16
No procedures for system configuration management	LOG_08
No use of norms or standards relating to information system development	ORG_04 ORG_04
No training plan for maintenance of new systems	ORG_14
Technology chosen without guarantee of continuity	ORG_13
Low maintenance budget	PER_13
Existence of obsolete components in the information processing infrastructure (development in languages no longer used, etc.)	ORG_13
Failure to comply with quality rules	PER_10
No standard or norm	PER_10
Failure to comply with development rules	PER_10
Insufficient training in the correct use of the information tool (disturbance of the system, installation of incompatible software, etc.)	PER_03 PER_12
Use of software or developments outside the organisation's norms and standards	PER_10
Maintenance fault	ORG_27
No cable layout plan	PHY_11
Maintenance or use of the equipment only possible if network supports are available	RES_02
System maintained or operated via the network	RES_02
No maximum response time for support guarantees	MAT_04

Use of an obsolete version of the operating system or applications	LOG_09 ORG_13
Use of an obsolete version of the messaging server	LOG_09 ORG_13
Use of an obsolete system	LOG_09
Use of a non-standard system	ORG_28
No monitoring of installation and maintenance procedures (configuration and parameter setting records)	ORG_04
No internal support tool	ORG_27

4.1.33 UNAUTHORISED USE OF EQUIPMENT

Vulnerability	Coverage
No management of licences or registration and activation measures	LOG_07
Possibility of installing a backdoor or Trojan horse in the operating system	LOG_08 LOG_13
Shared use of connection identifier	LOG_11
Resource sharing makes it easy for unauthorised persons to use the system	LOG_12
The system is connected to external networks	MAT_10
The equipment can be used for purposes other than those intended (development of software for use outside the organisation, etc.)	LOG_11 PER_03
Media available to everyone	MAT_07 ORG_15 ORG_30
Responsibilities for information systems security not dealt with in the internal regulations	ORG_14
No security policy for protecting the information processing infrastructure in the organisation's sites	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Managers have no contact with the expertise or technology watch departments	ORG_34
No awareness of the risks of sanction	ORG_37 PER_08
No contractual clauses relating to the use of IT equipment	ORG_04
No instructions concerning the use of IT equipment	ORG_04
Possibility of using the organisation's resources without supervision (self-service equipment, etc.)	LOG_11 ORG_33
No monitoring procedure	ORG_33
The security policy is not applied	ORG_18
No IT charter specifying the rules of use	ORG_04 PER_03
Unfamiliarity with security measures	PER_03 PER_11
Personnel not aware of the risks of sanction	PER_08
Rights assigned without legitimate need	PER_07
Obtaining an advantage	PER_08
Failure to comply with the IT charter specifying the rules of use	PER_03
Insufficient monitoring of material requirements for developing an application	ORG_32
No code of conduct	PER_08

No management of the equipment assets	PER_05
No procedures for checking authorisation of personnel entering the site or premises	PHY_07
No procedures for checking the identity of all persons entering the premises or zones	PHY_07
No logging of entry to the site	PHY_07
No measures to make communication lines and equipment secure	PHY_07
The equipment allows system resources to be used from outside	RES_01
The equipment can be accessed by everyone	RES_01
The equipment is connected to external networks	RES_01
The system can be used for purposes other than those intended	RES_06
The equipment can be used for purposes other than those intended	PER_03
No audit or supervision of accesses (for example inventory of accesses outside the organisation and types of data flow)	ORG_22
No access rules	LOG_11
The system is connected to external networks	RES_01 RES_03
The system can be accessed by everyone	LOG_11 ORG_01

4.1.34 FRAUDULENT COPYING OF SOFTWARE

Vulnerability	Coverage
No management of profile privileges (administrators, users, guest, etc.)	LOG_11 LOG_11
No management of licences or registration and activation measures	LOG_07
Tempting or popular software	ORG_04
Software can be easily copied	ORG_04
Proprietary operating system distributions can be easily copied	ORG_04
Tempting or popular operating system	ORG_04
Equipment allowing data to be recorded on media (floppy disc, ZIP disc, CD/DVD writer)	
Equipment allowing data to be recorded on media (floppy disc, ZIP disc, CD/DVD writer)	ORG_15
Lack of information concerning laws and regulations applicable to information processing	ORG_40 ORG_41
Responsibilities for information systems security not dealt with in the internal regulations	ORG_14
No licence monitoring policy imposed at the organisation's sites	LOG_07 ORG_38
No contractual clauses concerning the use of fraudulent copies of software	ORG_38 ORG_40
No IT charter specifying the rules of use	ORG_04 PER_03
No awareness of the risks of sanction	ORG_37 PER_08
No awareness or information concerning copyright law	ORG_40 ORG_41
No monitoring procedure	ORG_33
The security policy is not applied	ORG_18

No management support for application of the security policy	PER_13
Unfamiliarity with security measures	PER_03 PER_11
Obtaining an advantage	PER_08
Failure to comply with the IT charter specifying the rules of use	PER_03
Personnel not aware of the risk of sanction	PER_08
No procedures for checking the identity of all persons entering the premises or zones	PHY_07
No procedures for checking authorisation of personnel entering the site or the premises	PHY_07
No logging of entry to the site	PHY_07
The origin of applications is not checked before installation	ORG_20
The access system allows software storage	RES_01
The access system allows software downloads	RES_01

4.1.35 USE OF COUNTERFEIT OR COPIED SOFTWARE

Vulnerability	Coverage
No management of licences or registration and activation measures	LOG_07
Software can be easily copied	ORG_04
Tempting or popular software	ORG_04
Possibility of the systems operating with illegally copied or counterfeit operating systems	LOG_07 LOG_08 ORG_04
Responsibilities for information systems security not dealt with in the internal regulations	ORG_14
No licence monitoring policy imposed at the organisation's sites	LOG_07 ORG_38
Contract contains no clauses concerning identification and verification of the origin of the software.	ORG_38
No awareness or information concerning copyright law	ORG_40 ORG_41
No monitoring of product certification	ORG_20
No monitoring of product origin	ORG_20
No IT charter specifying the rules of use	ORG_04 PER_03
The security policy does not include reminding all personnel of their obligations and responsibilities in civil, criminal and regulatory matters.	ORG_40 ORG_41
No definition of privileges limiting the possibility of installing software on workstations	LOG_11 ORG_33
Personnel not aware of the risk of sanction	PER_08
Failure to comply with the IT charter specifying the rules of use	PER_03
Unfamiliarity with security measures	PER_03 PER_11
No management support for application of the security policy	PER_13
No product certification	LOG_06
No procedure for assessing products	ORG_20
No procedure and means of verifying the origin of the software (code signature, binary signature, etc.)	ORG_20
No logging of entry to the site	PHY_07

No procedures for checking authorisation of personnel entering the site or the premises	PHY_07
No procedures for checking the identity of all persons entering the premises or zones	PHY_07
The origin of applications is not checked before installation	ORG_20
The access system allows software storage	RES_01
The access system allows software downloads	RES_01

4.1.36 CORRUPTION OF DATA

Vulnerability	Coverage
No monitoring of data integrity	LOG_01
No procedure or system for authorising personnel to modify data	LOG_11
The remote maintenance link is permanently activated	LOG_12 RES_06
No restriction on software entry points	LOG_13
Applications are not checked before installation	LOG_06
No implementation of basic security rules applicable to the operating system and software	LOG_04
The operating system allows access to data (data base, etc.)	LOG_11
Possibility of remote system administration from any station	LOG_11
Possibility of remote administration of the system using non-encrypted administration tools	RES_02
The software allows access to data (content of hard disc, data base, etc.)	LOG_11
Connection passwords not sufficiently complex	ORG_10
The operating system is not checked before installation	LOG_06
Resource sharing makes it easy for unauthorised persons to use the system	LOG_12
Possibility of remote system administration	RES_01 RES_06
The SNMP layer is activated	LOG_12 RES_06
No data protection rules	ORG_15
The equipment can be booted from any peripheral (e.g. floppy disc, CD-ROM)	MAT_10
Obsolete hardware	ORG_13
No back-up redundancy or procedure	MAT_01 ORG_08
Wear of media	MAT_14
No means of protecting and monitoring data integrity	LOG_01 LOG_01
No rules and procedures for personnel authorisation	ORG_30
No authorisation management and monitoring policy imposed at the organisation's sites	LOG_11 ORG_14 ORG_15 ORG_38
No information protection policy imposed at the organisation's sites	ORG_15 ORG_38
Responsibilities for information systems security not dealt with in the internal regulations	ORG_14
No policy for authorising access to information	ORG_30
Accesses to the IS are not secured (gateways, intrusion detection, supervision of	ORG_30

security events, etc.)	
No contractual clauses relating to the protection of IT equipment	ORG_38
No monitoring of application of the security policy	ORG_22
No instructions concerning the use of IT equipment	ORG_04
No prevention and detection of viruses and other malicious programmes	ORG_06
No access control to information	ORG_15 ORG_30
No training plan concerning security issues	PER_02
No procedures for checking external floppy disks	ORG_06
No IT charter specifying the rules of use	ORG_04 PER_03
Failure to comply with the IT charter specifying the rules of use	PER_03
No protection and classification of information	ORG_15
Personnel not aware of the risk of sanction	PER_08
Unfamiliarity with security measures	PER_03 PER_11
Personnel susceptible to enticement	PER_02
Conflictual situation between persons	
No management support for application of the security policy	PER_13
No procedures for checking the identity of all persons entering the premises or zones	PHY_07
No procedures for checking authorisation of personnel entering the site or the premises	PHY_07
No logging of entry to the site	PHY_07
No measures to make communication lines and equipment secure	PHY_07
No physical and logical protection (partitioning, etc.)	RES_01 RES_02
Possibility of interfering with data transmitted via the communication media	RES_02
The network allows the system resources to be modified or adjusted	RES_01
The network makes it easy for unauthorised persons to use the resources	RES_01
No robust access control system	MAT_10 RES_01
No back-up procedure	ORG_08
The system allows remote deleting, modifying or installing of programmes	LOG_11
The system allows hostile software such as Trojan horses, viruses, worms, logic bombs, etc. to be introduced	ORG_06
The system allows asynchronous operation of certain parts or commands of the operating system (e.g. JavaScript components exploring the hard disc content)	LOG_04 LOG_11
No partitioning of communication networks	RES_02
The system allows asynchronous operation of certain parts or commands of the operating system to be exploited (e.g. automatic opening of attachments)	LOG_04
No audit or supervision of accesses	ORG_22
No access rules	LOG_11

4.1.37 ILLEGAL PROCESSING OF DATA

Vulnerability	Coverage
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	LOG_13

No encryption system	RES_02
Possibility of installing a backdoor or Trojan horse in the operating system	LOG_08 LOG_13
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	LOG_08
Possibility of installing a backdoor or Trojan horse in the operating system	
No physical protection	ORG_01 PHY_03 RES_01
No means of identifying the sensitivity of information contained on the media	ORG_15
Media available to everyone	MAT_07 ORG_15 ORG_30
Tempting equipment (trading value, technology, strategic)	MAT_07
Easily transported or removable media (e.g. floppy disc, ZIP disc, removable hard disc)	MAT_07
No means of encryption	ORG_15
No procedure and means for destruction	MAT_08
Lack of information concerning laws and regulations applicable to information processing	ORG_40 ORG_41
Managers have no contact with the expertise or technology watch departments	ORG_34
No subject in the internal regulations dealing with responsibilities for information systems security	ORG_14
No information protection policy imposed at the organisation's sites	ORG_15 ORG_38
No confidentiality clause in the contract	PER_09
No provisions for monitoring and sanctioning	ORG_37 PER_08
No instructions relating to incidents (detection, action, etc.)	ORG_24
No access control to information	ORG_15 ORG_30
Lack of awareness of individual responsibilities	ORG_14 PER_05
No one responsible for the protection of personal data and information	ORG_14 ORG_15
The security policy is not applied especially in relation to processing of personal information	ORG_18
Lack of personnel awareness	ORG_14 PER_05
No protection and audit of access to sensitive information	ORG_15 ORG_35
Personnel not aware of the risk of sanction	PER_08
No training to explain the conditions controlling the lawful use of information	PER_10
No protection and classification of information	ORG_15
Unfamiliarity with security measures	PER_03 PER_11
Access point allowing unlawful eavesdropping	RES_02
No identification of the system protection levels	ORG_22
No content monitoring	ORG_30
No audit or supervision of accesses	ORG_22

No management of access authorisation	LOG_11
The system makes it easy to disclose information to the outside	PER_02
The system is connected to external networks	RES_01 RES_03

4.1.38 ERROR IN USE

Vulnerability	Coverage
No explicit documentation on the application systems	ORG_28
Users lack competency	PER_12
No procedure for testing incoming goods and confirming their compliance with the specifications	LOG_06
No validation of keyed data entries	LOG_17
Lack of responsibility	ORG_14 PER_05
Application that is complex to use	LOG_17
No accessible user support	ORG_27
Non-intuitive software	LOG_17
Insufficient competency	ORG_14
No accessible support	ORG_27
No training in the use and maintenance of new software	ORG_14 PER_06 PER_12
Software that is complex to use	LOG_17
Equipment that is complex to use or not user-friendly	MAT_11
Incorrect operating conditions	MAT_14
Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	MAT_11 MAT_12
No labelling of media	MAT_06
Media are complex to use or not user-friendly	MAT_11
No monitoring of critical processes by the parent organisation	ORG_38
No double checking of critical processes	ORG_43
No training on the equipment or software used	PER_12
Lack of understanding of responsibilities	PER_05
No formalisation of responsibilities known by everyone	PER_05
Unfavourable work conditions	ORG_45
Lack of professionalism	PER_05
Failure to comply with instructions	PER_10
Users poorly trained or not trained at all	PER_12
Some highly sensitive operations can be performed by a single person	PER_07
No user documentation for existing applications	PER_12
Lack of motivation for work involving data keying	PER_05
Personnel not used to keying	PER_06
Unfavourable work environment (rooms too small, lack of storage areas, etc.)	PHY_12
No labelling of cables or cable layout plan	PHY_11
Technical rooms too cramped	PHY_12
No operating procedure	ORG_04
No up-to-date labelling and diagram of the architecture	MAT_06

No cable layout plan	PHY_11
Interface with technical characteristics specific to the country (e.g. different telephone connectors between France and the United Kingdom)	RES_04
Medium and supports with technical characteristics specific to their locality (e.g. different ADSL configuration parameters between France and the United Kingdom)	RES_04
No protection measures (read only, etc.)	LOG_11
No supervision tool	MAT_13

4.1.39 ABUSE OF RIGHTS

Vulnerability	Coverage
No audit policy	ORG_22
No back-up of event logs	ORG_08
No event logging	LOG_15
Assignment files too complex or unpractical	ORG_42
Connection passwords not sufficiently complex	ORG_10
Possibility of remote administration of the system using non-encrypted administration tools	RES_02
The password base of the operating system is decipherable	ORG_10
The SNMP layer is activated	LOG_12 RES_06
Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	LOG_14
The remote maintenance link is permanently activated	LOG_12 RES_06
Possibility of remote system administration	RES_01 RES_06
The operating system logs can be modified by anyone	LOG_11
Resource sharing makes it easy for unauthorised persons to use the system	LOG_12
The operating system can be accessed and used by everyone (e.g. connection via the guest account)	LOG_11
The operating system does not log system records or events	LOG_15
The operating system can be used to make anonymous connections	LOG_13
The operating system allows a session to be opened without password	LOG_13
Possibility of remote system administration from any station	LOG_11
Use of an obsolete version of the operating system or applications	LOG_09 ORG_13
The passwords entered for access to the operating system are decipherable	ORG_10
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	LOG_08
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	LOG_13
No physical protection	ORG_01 PHY_03 RES_01
No robust access control system	MAT_10 RES_01
No audit of physical access control procedures	ORG_22
No authorisation management and monitoring policy imposed at the organisation's	LOG_11

sites	ORG_14 ORG_15 ORG_38
Responsibilities for information systems security not dealt with in the internal regulations	ORG_14
Managers have no contact with the expertise or technology watch departments	ORG_34
No contractual clauses setting out the responsibilities of both parties	ORG_38
No definition of the right to know	ORG_33
No provisions for monitoring and sanctioning	ORG_37 PER_08
No regulation defining rights	ORG_33
Assignment of user rights is not clearly defined	ORG_14
User grant rights are not controlled.	LOG_11
Personnel categories with higher access privileges	PER_05
No management support for application of the security policy	PER_13
Some highly sensitive operations can be performed by a single person	PER_07
Obtaining an advantage	PER_08
The notion of right is not defined for the personnel	PER_05
No procedures for checking authorisation of personnel entering the site or the premises	PHY_07
No physical and logical protection	RES_01
The principle of least privilege is not applied	LOG_11
Resources can be used without tracking	RES_03
The system can be accessed by everyone	LOG_11 ORG_01

4.1.40 FORGING OF RIGHTS

Vulnerability	Coverage
No audit policy	ORG_22
No back-up of event logs	ORG_08
No event logging	LOG_15
The operating system logs can be modified by anyone	LOG_11
The operating system allows a session to be opened without password	LOG_13
The operating system can be used to make anonymous connections	LOG_13
The operating system does not log system records or events	LOG_15
The operating system can be accessed and used by everyone (e.g. connection via the guest account)	LOG_11
Resource sharing makes it easy for unauthorised persons to use the system	LOG_12
The password base of the operating system is decipherable	ORG_10
The SNMP layer is activated	LOG_12 RES_06
Assignment files too complex or unpractical	ORG_42
Possibility of remote administration of the system using non-encrypted administration tools	RES_02
Possibility of remote system administration	RES_01 RES_06
The remote maintenance link is permanently activated	LOG_12 RES_06

The passwords entered for access to the operating system are decipherable	ORG_10
Connection passwords not sufficiently complex	ORG_10
Use of an obsolete version of the operating system or applications	LOG_09 ORG_13
Possibility of the system being subjected to badly formed requests and data (e.g. buffer overflow)	LOG_14
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	LOG_08
Possibility of remote system administration from any station	LOG_11
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	LOG_13
The equipment is connected to external networks	MAT_10
No robust access control system	MAT_10 RES_01
No partitioning of equipment	MAT_10
No protection of media	ORG_30
No audit of physical access control procedures	ORG_22
Managers have no contact with the expertise or technology watch departments	ORG_34
No rules and procedures for personnel authorisation	ORG_30
No awareness of the risks of sanction	ORG_37 PER_08
Responsibilities for information systems security not dealt with in the internal regulations	ORG_14
No monitoring procedure	ORG_33
Possibility of using the organisation's resources without supervision (self-service equipment, etc.)	LOG_11 ORG_33
No protection of spaces dedicated to information exchange or sharing	ORG_30
No procedure for personnel authorisation	LOG_11 ORG_30
No climate of trust between individuals	ORG_37 PER_05
The security responsibilities concerning authorisation management are not formalised.	ORG_14 ORG_15
Personnel receive no communication or information concerning authorisation procedures	ORG_41
No procedure for passing up information in the event of detection	ORG_24
The security policy is not applied	ORG_18
Inappropriate organisation	ORG_14
Rights assigned without legitimate need	PER_07
Conflictual situation between persons	
No code of conduct	PER_08
Obtaining an advantage	PER_08
Some highly sensitive operations can be performed by a single person	PER_07
No management support for application of the security policy	PER_13
Missions not suited to the personnel	ORG_14
No procedures for checking authorisation of personnel entering the site or the premises	PHY_07
No physical and logical protection (partitioning, etc.)	RES_01 RES_02

No network partitioning	RES_01 RES_02
The interfaces are connected to external networks	RES_01
The supports and medium are connected to external networks	RES_01
Technical characteristics can be modified (e.g. MAC address of an Ethernet card)	LOG_11
No physical protection	ORG_01 PHY_03 RES_01
The network allows the system resources to be modified or adjusted	RES_01
Presence of protocol that has no authentication function	RES_03
The interfaces can be accessed by everyone	RES_01
The network makes it easy for unauthorised persons to use the resources	RES_01
The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)	RES_03
The system can be accessed by everyone	LOG_11 ORG_01
Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	LOG_14
Applications are not checked before installation	LOG_06
The messaging system can be accessed from Internet	RES_01
Use of an obsolete version of the messaging server	LOG_09 ORG_13

4.1.41 DENIAL OF ACTIONS

Vulnerability	Coverage
No audit policy	ORG_22
No back-up of event logs	ORG_08
No event logging	LOG_15
The operating system does not log system records or events	LOG_15
The SNMP layer is activated	LOG_12 RES_06
Possibility of remote administration of the system using non-encrypted administration tools	RES_02
Assignment files too complex or unpractical	ORG_42
Connection passwords not sufficiently complex	ORG_10
The passwords entered for access to the operating system are decipherable	ORG_10
The password base of the operating system is decipherable	ORG_10
The operating system can be used to make anonymous connections	LOG_13
Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	LOG_14
Possibility of remote system administration from any station	LOG_11
Use of an obsolete version of the operating system or applications	LOG_09 ORG_13
The operating system can be accessed and used by everyone (e.g. connection via the guest account)	LOG_11
Possibility of remote system administration	RES_01 RES_06
The operating system logs can be modified by anyone	LOG_11
Possibility of booting several operating systems on the same machine (e.g.	LOG_08

access to NTFS partitions via Linux)	
The operating system allows a session to be opened without password	LOG_13
The remote maintenance link is permanently activated	LOG_12 RES_06
Resource sharing makes it easy for unauthorised persons to use the system	LOG_12
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	LOG_13
No tracking and auditing system	ORG_39 RES_03
The equipment can be accessed and used by everyone	MAT_10
Media available to everyone	MAT_07 ORG_15 ORG_30
No procedure for access to classified information	ORG_15
Change of the organisation's policy or strategy	ORG_14 ORG_33
No definition of responsibilities	ORG_14
Responsibilities for information systems security not dealt with in the internal regulations	ORG_14
No disciplinary procedures	ORG_37
High political / economic stakes	ORG_31
No global policy for managing and archiving tracks and other elements of proof	ORG_39
No contractual clause concerning the definition of communication and exchange procedures	ORG_03 ORG_38
No mutual checking of codes	ORG_20 ORG_38
Penalty or sanction clause out of proportion or not suited to the context	ORG_38 ORG_37
No mechanism for monitoring actions, logs and alerts	ORG_39
Possibility of using the organisation's resources without supervision (self-service equipment, etc.)	LOG_11 ORG_33
No hierarchical organisation or reporting procedure	ORG_21
Audit functions are not separate from monitoring functions	ORG_22 PER_07
No management support for application of the security policy	PER_13
Obtaining an advantage	PER_08
Lack of confidence in the organisation	
Responsibility of each person not known	PER_05
Conflictual situation between persons	
No history recording persons entering and leaving	PHY_07
The relays can be accessed by everyone	RES_01
The medium allows system resources to be used from outside	RES_01
The supports and medium can be accessed by everyone and are active by default (e.g. RJ45 connectors intermingled)	RES_01
The network makes it easy for unauthorised persons to use the resources	RES_01
The protocol does not allow certain identification of the sender	RES_03
The network allows the system resources to be modified or adjusted	RES_01
The protocol does not allow acknowledgement of receipt to be sent	RES_03
Resources can be used without tracking	RES_03

The access system does not log tracks of its operation	ORG_39
Access to the tracking system is not protected	LOG_11
The system can be accessed by everyone (e.g. does not authenticate client stations or users)	LOG_11
The system is connected to external networks	RES_01 RES_03

4.1.42 BREACH OF PERSONNEL AVAILABILITY

Vulnerability	Coverage
Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	MAT_11 MAT_12
No archiving procedure	ORG_07
Unfavourable industrial relations	
Political / economic conflict between the organisation's home country and its host country	ORG_31
No clause or procedures for transfer of knowledge	ORG_38 PER_06
The organisation's financial or technological continuity is not secure	ORG_13
No continuity clause for service provision	ORG_16 ORG_38
No personnel protection team	ORG_45
Viral epidemic in the locality	PER_04
No procedures for transfer of knowledge	PER_06
The organisation's activity is impaired by its industrial relations	
No awareness and training programme for processes relating to continuity of professional activities	ORG_16 PER_10
No process for managing the continuity of the organisation's professional activities	ORG_16
The organisation is under-sized	ORG_14 PER_04
No substitutes for strategic personnel	PER_04
No substitute organisation for sensitive functions	ORG_14 PER_04
No process for managing the continuity of the project team's professional activities	ORG_16
No document base for rules and procedures	ORG_41
Unavailability arising from a competition factor	PER_05
Unavailability caused by illness	PER_04
Unavailability caused by absenteeism	PER_04 PER_05
Unavailability caused by third parties (physical aggression, hostage taking, etc.)	PER_04
Social problems	
Conflictual industrial relations	
Difficult industrial relations possibly resulting in transport strikes	PHY_04
Specialised personnel accommodated in remote rooms	PHY_04
Personnel living a long way from the premises	PHY_04
Possible harm to personnel using the equipment (wireless transmission, emanations, etc.)	MAT_12

5 Proposed coverage of generic security objectives by security requirements

The following tables are used to identify at a glance the generic security requirements liable to satisfy each generic security objective (the codes of which correspond to those of the previous parts).

5.1 MAT : Hardware

MAT_01	
Coverage	BGC_INT.1.1 BGC_PRE.1.1 CGS_GSS.1.1 CGS_SVG.1.3 CGS_SVG.1.4 CGS_SVG.1.5 CGS_SVG.1.6 CGS_SVG.1.7 CGS_SVG.1.8 CGS_SVG.1.9 FRU_FLT.1.1 FRU_FLT.2.1

MAT_02	
Coverage	BGC_INT.1.1 CGS_SVG.1.1 CGS_SVG.1.2

MAT_03	
Coverage	BMA_MAA.2.1 BPE_SEM.1.1

MAT_04	
Coverage	BGC_MSS.1.1 CGS_ARC.1.1 CGS_ARC.1.2

MAT_05	
Coverage	CAR_AAR.1.1 CAR_PAR.1.1 FRU_FLT.1.1

MAT_06	
Coverage	BCM_RLC.1.1

MAT_07	
Coverage	BCM_RLC.1.1 BMA_REU.2.1 BPE_SEM.1.1 BPE_SEM.5.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BSP_RIS.5.1 BSP_RIS.5.2 CET_EGT.1.10

	CET_EGT.1.8 CET_EGT.1.9 CET_EGT.2.3 CET_EGT.3.1 CGS_PPS.2.1 CGS_PPS.3.1 CGS_PPS.3.2 FIA_UAU.1.2/2.1 FIA_UAU.6.1 FIA_UID.1.2/2.1
MAT_08	
Coverage	BGC_INT.1.1 BGC_MSS.2.1 CGS_SVG.1.2
MAT_09	
Coverage	BDM_ESS.1.1 BGC_PRS.1.1 CAR_AAR.1.1 CEI_ABS.1.5
MAT_10	
Coverage	BGC_EIL.2.1 BGC_MSS.3.1 BGC_PRE.4.1 BPE_SEM.1.1 BPE_ZOS.2.1 CGS_GLI.2.1 FTA_TAB.1.1
MAT_11	
Coverage	BSP_FOU.2.1 CEI_CDT.2.1 CEI_CDT.2.2
MAT_12	
Coverage	BSP_FOU.2.1 CEI_CDT.2.1 CEI_CDT.2.2
MAT_13	
Coverage	CGS_GSU.1.1 CGS_GSU.1.3 CGS_SUP.1.1
MAT_14	
Coverage	CGS_OML.1.1
MAT_15	
Coverage	BGC_PRS.2.1

5.2 LOG : Software

LOG_01	
Coverage	BDM_COC.3.1 FDP_ITT.3.1 FDP_ITT.3/4.2 FDP_SDI.1/2.1 FDP_SDI.2.1 FPT_ITI.1/2.2 FPT_ITT.3.1 FPT_ITT.3.2 FPT_TST.1.2

LOG_02	
Coverage	BDM_SED.1.1 BDM_SED.2.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SED.5.1 BGC_PRE.2.1 BGC_PRS.2.1 CDO_SDC.1.2 CGS_GMA.6.1

LOG_03	
Coverage	BCO_RPS.2.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.4.1 BGC_PRE.2.1 BGC_PRE.2.2 BMA_SAS.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_EIP.1.6

LOG_04	
Coverage	CGS_CSR.1.2 FMT_MSA.3.1

LOG_05	
Coverage	

LOG_06	
Coverage	BDM_SED.4.1 BDM_SFS.1.1 BGC_PLM.1.1 BGC_PRS.2.1 CGS_OML.1.1 CGS_OML.1.2 CGS_PPS.2.4

LOG_07	
Coverage	BCM_RLC.1.1 BCO_CEL.3.1 CGS_GLI.1.1 CGS_GLI.1.2 CGS_GLI.1.3 CGS_GLI.1.4

LOG_08

Coverage	BCM_RLC.1.1 BCO_RPS.2.1 BDM_SED.1.1 BDM_SED.3.1 BDM_SED.4.1 BGC_PRE.2.1 BGC_PRE.2.2 BGC_PRS.2.1 BMA_MAS.3.1 CDO_SDC.1.1 CGS_PPS.1.1 CGS_PPS.2.1 CGS_PPS.2.3 CGS_PPS.2.4 FIA_UAU.7.1 FPT_RVM.1.1 FPT_SEP.1.1

LOG_09	
Coverage	BGC_PRE.1.1 CDO_APP.1.1 CDO_APP.1.2 CEI_CDT.1.1 CEI_CDT.1.2

LOG_10	
Coverage	BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.3.1 FPT_STM.1.1

LOG_11	
Coverage	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SFS.1.1 BGC_EIL.6.1 BGC_MSS.2.1 BGC_MSS.3.1 BGC_PRE.2.1 BGC_PRS.2.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAA.1.1 BMA_MAR.1.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_MAS.5.1 BPE_SEM.6.1 BPS_PSI.1.5 CGS_CSR.1.2 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.4

	CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GDH.2.1 CGS_GDT.1.1 CGS_GLI.2.1 CGS_PAI.1.1 CGS_PAI.1.2 CGS_PAI.1.3 CGS_PEP.1.1 CGS_PPS.2.1 CGS_PPS.2.5 FDP_RIP.1.1 FDP_RIP.2.1 FMT_MOF.1.1 FMT_MSA.1.1 FMT_MSA.3.2 FMT_MTD.1.1 FMT_MTD.2.1
LOG_12	
Coverage	FAU_SAA.2.3
LOG_13	
Coverage	BDM_SED.4.1 BMA_MAS.3.1 BMA_MAS.7.1 BMA_MAS.8.1 CGS_GDH.1.2 CGS_GDH.2.1 CGS_PPS.2.3 CGS_PPS.2.4 FIA_UAU.7.1 FTA_SSL.1.1 FTA_SSL.2.1 FTA_SSL.3.1
LOG_14	
Coverage	BDM_SSA.1.1 BGC_EIL.4.1 CAR_AAR.1.1 CGS_CME.1.1 CGS_PPS.2.4 FRU_FLT.1.1
LOG_15	
Coverage	BMA_SAS.1.1 CET_EGT.1.6 FAU_GEN.1.1 FAU_GEN.1.2
LOG_16	
Coverage	BMA_MAS.7.1 BMA_MAS.8.1 CIS_ADL.1.1 FTA_SSL.1.1 FTA_SSL.2.1 FTA_SSL.3.1
LOG_17	
Coverage	BGC_EIL.4.1

	BGC_EIL.5.1 CGS_PPS.2.3

5.3 RES : Network

RES_01	
Coverage	BCO_CEL.5.1 BDM_COC.2.1 BDM_COC.4.1 BGC_EIL.1.1 BGC_EIL.4.1 BGC_PLM.1.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1 BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.3.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.6.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_REU.2.1 BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 CAR_PAR.1.1 CET_EGT.1.1 CGS_CSR.1.1 CGS_CSR.1.2 CGS_CSR.1.3 CGS_GDA.1.1 CGS_GDA.3.1 CGS_GDA.3.2 CGS_GDH.1.1 CIS_PSI.1.1 FMT_MOF.1.1 FMT_MSA.1.1 FMT_MSA.3.2 FMT_MTD.1.1 FMT_MTD.2.1 FPT_ITA.1.1 FPT_ITI.1/2.1 FPT_ITI.1/2.2 FPT_ITI.2.3 FPT_ITT.3.1 FPT_ITT.3.2 FTA_TAB.1.1 FTA_TSE.1.1

RES_02	
Coverage	BDM_COC.1.1 BDM_COC.2.1 BDM_COC.4.1 BDM_COC.5.1 BGC_GER.1.1 BGC_PRE.4.1 BGC_PRS.1.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1

	BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.6.1 BMA_MAR.7.1 BPE_SEM.1.1 BPE_SEM.3.1 BPE_ZOS.2.1 CAR_PAR.1.1 CGS_CSR.1.2 CGS_PPS.1.2 CGS_PPS.1.3 FCO_NRO.2.1 FCS_COP.1.1 FDP_ITT.1/2.1 FDP_UCT.1.1 FPT_ITC.1.1 FPT_ITT.1/2.1 FTA_TAB.1.1
RES_03	
Coverage	BDM_COC.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BMA_MAR.4.1 BMA_MAS.1.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_MAS.6.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BPE_SEM.1.1 CGS_GDA.1.3 FAU_STG.1/2.1 FAU_STG.1/2.2 FAU_STG.2.3 FCO_NRO.1.1 FCO_NRO.1.2 FCO_NRO.1.3 FCO_NRO.2.1 FCO_NRR.1.1 FCO_NRR.1.2 FCO_NRR.1.3 FCO_NRR.2.1 FDP_UCT.1.1 FIA_UAU.1.2/2.1 FTA_TAB.1.1
RES_04	
Coverage	BGC_PRS.2.1 BMA_MAR.8.1 CGS_PPS.2.2 CGS_PPS.2.3 CIS_PSI.1.2
RES_05	
Coverage	BMA_MAR.8.1 BPE_SEM.3.1
RES_06	
Coverage	BDM_COC.4.1

	BGC_PLM.1.1 BMA_GAU.2.1 BMA_MAR.5.1

5.4 PER : Personnel

PER_01	
Coverage	BGC_EIL.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_EIL.6.1 BGC_EIL.7.1 BGC_MSS.1.1 BMA_IMT.1.1 BMA_IMT.2.1 BPE_SEM.5.1 BSP_FOU.1.1 CCS_CSG.1.3

PER_02	
Coverage	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_EIL.6.1 BGC_MSS.2.1 BOS_ISI.3.1 BPE_MMG.2.1 BPE_SEM.6.1 BPS_PSI.1.5 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCS_SRI.1.1 CET_EGT.2.3 CFO_SPS.1.1 CGS_CIR.1.1 CGS_CIR.1.2 CGS_CIR.1.3 CRR_SEN.1.1

PER_03	
Coverage	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_SED.1.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SFS.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_INT.3.1 BGC_MSS.3.1 BGC_PLM.1.1 BGC_PRE.1.1

	BGC_PRE.2.1 BGC_PRE.2.2 BMA_GAU.2.1 BMA_MAS.5.1 BMA_REU.1.1 BPS_PSI.1.4 BPS_PSI.1.5 BSP_FOU.1.1 BSP_FOU.2.1 BSP_RIS.1.1 BSP_RIS.3.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CCS_CHI.1.1 CCS_CSG.1.1 CCS_CSG.1.2 CCS_CSG.1.3 CCS_CSG.1.4 CFO_SPS.1.1 CGI_GIS.1.1 CGI_GIS.1.8 CGS_GDH.1.2 CGS_GDH.2.1 CGS_GMP.1.1 CGS_GMP.1.3 CGS_OML.1.2 CGS_PPS.2.1 CGS_PPS.2.3 CPD_DGL.1.1 CPD_DGL.1.2 CRR_SEN.1.1
PER_04	
Coverage	BSP_RIS.5.1 BSP_RIS.5.2 CFO_FRS.1.1 CFO_FRS.1.2 CFO_FRS.1.3 CFO_FRS.1.4 CFO_FRS.1.5 CRH_DDE.1.1 CRH_DDE.1.2 CRH_PDP.1.1
PER_05	
Coverage	BGC_PRS.1.1 BOS_ISI.3.1 BOS_SAT.1.3 BPS_PSI.1.3 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CDO_SDC.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CFO_FRS.1.1 CFO_FRS.1.2

	CFO_FRS.1.3 CFO_FRS.1.4 CFO_FRS.1.5 CFO_SPS.1.1 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3 CGI_GIS.3.4 CGI_GIS.3.5 CGI_GIS.3.6 CGS_GDH.1.2 CGS_HSI.1.1 CGS_HSI.1.2 CGS_PAI.2.1 CGS_PAI.2.3 CPS_PAQ.2.1 CPS_PAQ.2.2 CRH_DDE.1.1 CRH_DDE.1.2
PER_06	
Coverage	BSP_FOU.1.1 BSP_FOU.2.1 CDO_APP.1.1 CDO_APP.1.2 CFO_FRS.2.1 CFO_FRS.2.2 CFO_FRS.2.3 CFO_FRS.2.4 CPS_PAQ.3.1
PER_07	
Coverage	BOS_ISI.7.1 CGS_GDH.1.1 CGS_GDH.1.3 CGS_GDH.1.4 CGS_GDH.1.5 CGS_GDH.1.7 CGS_GPC.2.1 CGS_GPC.2.2 CGS_GPC.2.3 CGS_GPC.2.4
PER_08	
Coverage	BMA_MAS.6.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.3.1 CCS_CHI.1.1
PER_09	
Coverage	BGC_PRE.6.1 BOS_SOT.1.1 BOS_SOT.1.2 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.3.1 CFO_SPS.1.1 CPD_DGL.1.1 CPD_DGL.1.2
PER_10	
Coverage	BCM_CLI.1.1

	BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_SED.4.1 BDM_SFS.1.1 BDM_SFS.3.1 BMA_GAU.2.1 BMA_MAS.5.1 BPS_PSI.1.3 BPS_PSI.1.4 BPS_PSI.1.5 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CFO_SPS.1.1 CGS_OML.1.2 CGS_PPS.2.1 CGS_PPS.2.3 CPS_DEV.1.1 CPS_DEV.1.2 CPS_PAQ.1.1 CPS_PAQ.1.2 CPS_PAQ.1.3 CPS_PAQ.1.6
PER_11	
Coverage	BCA_AGC.1.1 BCA_AGC.5.1 BGC_INT.3.1 BPS_PSI.1.4 BSP_FOU.1.1 BSP_RIS.1.1 BSP_RIS.3.1 CCS_SIN.2.1 CCS_SIN.2.2 CCS_SIN.2.3 CCS_SIN.3.4 CCS_SIN.3.5 CCS_SSE.1.2 CCS_SSE.1.3 CCS_SSE.1.7 CGI_GDC.1.4 CGI_GDC.3.1 CGI_GDC.3.2 CGI_GDC.3.3 CGI_GDC.3.4 CGI_GDC.3.5 CGI_GDC.3.6 CGI_GIS.1.8 CRR_SEN.1.2
PER_12	
Coverage	BSP_FOU.1.1 BSP_FOU.2.1 CCS_CSG.1.2 CDO_APP.1.1 CDO_APP.1.2

	CGS_GMA.2.1
PER_13	
Coverage	BOS_ISI.1.1 BPS_PSI.1.1 CGS_GMA.5.1

5.5 PHY : Site

PHY_01	
Coverage	BGC_PRE.6.1 BPE_SEM.2.1 BPE_SEM.4.1 BSP_FOU.2.1 CAR_AAR.1.1 CDS_DES.1.1 CDS_DES.1.2 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CGS_GSS.1.1 CGS_GSS.1.2 CIS_ADL.2.1 CIS_MPP.1.1 CIS_MPP.1.2 CIS_MPP.1.3

PHY_02	
Coverage	BPE_MMG.1.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.4.1 CIS_ADL.1.1 CIS_ADL.1.2

PHY_03	
Coverage	BOS_SAT.1.2 BPE_SEM.1.1 BPE_SEM.2.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CEI_ERS.1.1 CET_EGT.1.1 CGS_PDI.1.1 CIS_ADL.1.2 CIS_ADL.2.1 CIS_ADL.2.2 CIS_MPP.1.2 CIS_MPP.2.2 CIS_MPP.3.1 CIS_MPP.3.2 CIS_MPP.3.3 CIS_MPP.3.4 CIS_PSI.1.1 CIS_PSI.1.2 CIS_SSI.1.2 CIS_ZOS.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1

PHY_04

Coverage	CIS_ADL.2.1 CIS_CDL.1.1 CIS_SSI.1.1 CIS_SSI.1.2 CIS_SSI.1.3 CIS_SSI.1.4 CRH_PDP.1.1 CRH_PDP.1.2 CRH_PDP.1.3 CRR_ETU.1.1 CRR_ETU.1.2 CRR_ETU.2.1 CRR_ETU.2.2

PHY_05

Coverage	BGC_GER.1.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.4.1 CIS_ADL.1.1 CIS_ADL.1.2 CPD_DGL.1.1

PHY_06

Coverage	CEI_ERS.1.1

PHY_07

Coverage	BGC_GER.1.1 BGC_INT.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.4.1 CET_EGT.1.3 CET_EGT.1.5 CET_EGT.1.6 CET_EGT.3.1 CET_EGT.3.2 CET_EGT.3.3 CET_EGT.3.4 CET_EGT.3.5 CIS_ADL.1.1 CIS_ADL.3.1 CIS_CSI.1.1 CIS_MPP.1.1

PHY_08

Coverage	CCS_CSG.1.2

PHY_09

Coverage	CIS_CSI.1.1 CIS_CSI.1.2 CIS_MPP.2.1 CIS_MPP.2.2

PHY_10

Coverage	BPE_SEM.4.1 CCS_RGI.1.1 CGS_GMA.1.1 CGS_GMA.1.2

	CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CIS_ADL.2.1 CIS_CSI.1.1 CIS_CSI.2.1 CIS_MPP.2.2 CIS_PSI.1.1 CIS_PSI.1.2
PHY_11	
Coverage	CIS_ADL.3.1 CIS_CSI.1.1
PHY_12	
Coverage	CIS_ADL.2.3 CRH_CDT.1.1

5.6 ORG : Organisation

ORG_01	
Coverage	BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 CET_EGT.1.1 CET_EGT.2.3 CET_EGT.3.1 CGS_GDH.1.2 CGS_GDH.2.1 CIS_PSI.1.1 CIS_PSI.1.2 FCO_NRO.2.1

ORG_02	
Coverage	BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CET_EGT.1.10 CET_EGT.1.8 CET_EGT.1.9 CGS_PDI.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3

ORG_03	
Coverage	BGC_EIL.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.7.1

ORG_04	
Coverage	BCM_CLI.2.1 BCM_RLC.1.1 BCO_CEL.2.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_SED.3.1 BDM_SED.5.1 BDM_SFS.1.1 BDM_SFS.2.1 BDM_SFS.3.1 BGC_EIL.5.1 BGC_MSS.1.1 BGC_MSS.3.1 BGC_PRE.1.1 BGC_PRE.2.2 BMA_IMT.2.1 BOS_SAT.1.2 BOS_SAT.1.5 BOS_SAT.2.1 BPE_MMG.1.1 BPE_MMG.2.1 BPE_SEM.1.1 BPE_SEM.2.1 BPE_SEM.3.1 BPE_SEM.3.2

	BPE_SEM.5.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CCS_CHI.1.1 CCS_CSG.1.1 CCS_CSG.1.2 CCS_CSG.1.3 CCS_CSG.1.4 CCS_CSG.1.5 CCS_CSG.1.6 CCS_CSG.1.7 CDO_SDC.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_EIP.1.6 CGS_GLI.1.4 CGS_GLI.2.1 CGS_PDI.1.1 CGS_PPS.2.1 CGS_PPS.2.5 CPS_DEV.1.1 CPS_DEV.1.2 CPS_PPT.1.1 CPS_PPT.1.2 CPS_PPT.1.3 CPS_PPT.1.4 CPS_PPT.1.5 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_05	
Coverage	CDO_SDC.1.2 CGS_ARC.1.7 CGS_SVG.1.7
ORG_06	
Coverage	BDM_SED.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_MSS.1.1 BGC_PLM.1.1 CGS_CME.1.1 CGS_OML.1.1 CGS_OML.1.3 CGS_PPS.2.3 CGS_PPS.2.4 CPS_PPT.1.1 CPS_PPT.1.2 CPS_PPT.1.3 CPS_PPT.1.4 CPS_PPT.1.5
ORG_07	

Coverage	BGC_PRE.1.1 CGS_ARC.1.3 CGS_ARC.1.4 CGS_ARC.1.5 CGS_ARC.1.6 CGS_ARC.1.7 CGS_ARC.1.8 CGS_ARC.1.9

ORG_08

Coverage	BGC_INT.1.1 BGC_PRE.1.1 CGS_GLI.1.2 CGS_GSS.1.1 CGS_SVG.1.1 CGS_SVG.1.2 CGS_SVG.1.3 CGS_SVG.1.4 CGS_SVG.1.5 CGS_SVG.1.6 CGS_SVG.1.7 CGS_SVG.1.8 CGS_SVG.1.9

ORG_09

Coverage	BCA_AGC.1.1 BCA_AGC.3.1 BCA_AGC.5.1 BGC_MSS.2.1 BGC_PRS.1.1 BGC_PRS.2.1 BPE_SEM.6.1 BSP_FOU.1.1 CCS_CSG.1.2 CDO_APP.1.1 CDO_APP.1.2 CDS_DES.1.1 CEI_ABS.1.5 CFO_FRS.2.2 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3 CGS_CSR.1.2 CRH_DDE.1.1 CRH_DDE.1.2 FDP_RIP.1.1 FDP_RIP.2.1

ORG_10

Coverage	BMA_MAS.4.1 BMA_REU.1.1 BMA_REU.2.1 CGS_GMP.1.1 CGS_GMP.1.2 FIA_SOS.1.1 FIA_SOS.2.1 FIA_SOS.2.2

ORG_11

Coverage	

ORG_12

Coverage	BGC_EIL.4.1

	CCS_CSG.1.1 CCS_CSG.1.2 CFO_SPS.1.1 CFO_SPS.1.2 CGS_CME.1.1 CGS_CSR.1.2
ORG_13	
Coverage	BGC_PRS.2.1 BPE_SEM.4.1 CCC_RGF.1.1 CCC_RGF.1.2 CEI_CDT.1.1 CEI_CDT.1.2
ORG_14	
Coverage	BCM_CLI.1.2 BDM_SSA.3.1 BGC_EIL.1.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_SAS.2.1 BOS_ISI.3.1 BPS_PSI.1.3 BSP_FOU.1.1 BSP_FOU.2.1 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCS_SRI.1.1 CDO_APP.1.1 CDO_APP.1.2 CFO_FRS.1.2 CFO_FRS.1.3 CFO_FRS.1.5 CGI_GDC.2.3 CGI_GDC.2.4 CGI_GDC.2.5 CGI_GDC.3.3 CGI_GDC.3.5 CGI_GDC.3.6 CGI_GDC.4.5 CGI_LCI.1.4 CGI_LCI.1.5 CGI_LCI.1.6 CGI_LCI.1.7 CGS_CIR.1.3 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GDH.2.1 CGS_GDH.2.2 CGS_GMA.2.1 CGS_OES.1.1 CGS_OES.1.2

	CGS_OES.1.3 CGS_PAI.1.1 CGS_PAI.1.2 CGS_PAI.1.3 CRH_DDE.1.1 CRH_DDE.1.2 CRH_QDP.1.1

ORG_15

Coverage	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_COC.2.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.7.1 BGC_GER.1.1 BGC_MSS.1.1 BGC_MSS.2.1 BGC_MSS.3.1 BMA_IMT.2.1 BMA_MAA.1.1 BPE_MMG.1.1 BPE_MMG.2.1 BPE_SEM.6.1 BPS_PSI.1.5 BSP_SPR.3.1 CGS_CIR.1.1 CGS_CIR.1.2 CGS_GDH.1.1 CGS_GDH.1.4 CGS_GMR.1.1 CGS_GMR.1.2 CPD_DGL.1.1 FDP_RIP.1.1 FDP_RIP.2.1

ORG_16

Coverage	BCA_AGC.1.1 BCA_AGC.2.1 BCA_AGC.3.1 BCA_AGC.4.1 BCA_AGC.5.1 BGC_PRE.3.1 BSP_RIS.1.1 CCS_SIN.2.1 CCS_SIN.2.3 CCS_SIN.3.1 CCS_SIN.3.2 CCS_SIN.3.4 CCS_SIN.3.5 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GSS.1.3 CGS_GSS.1.4 CGS_GSS.2.1 CGS_GSS.2.2

ORG_17

Coverage	CCS_SIN.1.1 CCS_SIN.1.2

	CCS_SIN.1.3 CCS_SIN.1.4 CCS_SIN.2.1 CCS_SIN.3.1 CCS_SIN.3.2
ORG_18	
Coverage	BCO_CEL.4.1 BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BPS_PSI.1.4 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1
ORG_19	
Coverage	
ORG_20	
Coverage	BDM_ESS.1.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.4.1 BDM_SED.5.1 BDM_SFS.3.1 BGC_MSS.1.1 BGC_PLM.1.1 BGC_PRS.2.1 BOS_SAT.1.3 CGS_OML.1.1 CGS_OML.1.2 CGS_OML.1.3 CGS_PPS.2.3
ORG_21	
Coverage	BOS_ISI.1.2 BSP_RIS.1.1 BSP_RIS.4.1 CGI_GIS.2.1 CGI_GIS.2.2 CGI_GIS.2.3 CGI_GIS.2.4 CGI_GIS.2.5 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3
ORG_22	
Coverage	BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_COC.4.1 BGC_PRE.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BOS_ISI.7.1 BOS_SAT.1.1 CCS_SIN.3.3 CCS_SSE.1.1 CIS_CSI.1.3

	CPD_INP.1.1 FAU_ARP.1.1 FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1 FAU_SAA.1.1 FAU_SAA.1.2 FAU_SAA.2.1 FAU_SAA.2.2 FAU_SAA.2.3 FAU_SAA.3.1 FAU_SAA.3.2 FAU_SAA.3.3 FAU_SAA.4.1 FAU_SAA.4.2 FAU_SAA.4.3
ORG_23	
Coverage	BCO_RPS.1.1 BCO_RPS.1.2 BPE_ZOS.1.1 CIS_CSI.1.1 CIS_CSI.1.2 CIS_PSI.1.1 CIS_PSI.1.2 CIS_PSI.1.3
ORG_24	
Coverage	BGC_PRE.1.1 BGC_PRE.3.1 BSP_RIS.1.1 BSP_RIS.2.1 CCS_SIN.2.1 CCS_SIN.2.3 CCS_SIN.3.1 CCS_SIN.3.2 CCS_SIN.3.4 CCS_SIN.3.5 CCS_SSE.1.1 CCS_SSE.1.2 CCS_SSE.1.3 CCS_SSE.1.4 CCS_SSE.1.5 CCS_SSE.1.6 CCS_SSE.1.7 CGI_GDC.1.1 CGI_GDC.1.2 CGI_GDC.1.3 CGI_GDC.1.4 CGI_GDC.2.1 CGI_GDC.2.2 CGI_GDC.2.6 CGI_GDC.3.1 CGI_GDC.3.2 CGI_GDC.3.4 CGI_GDC.4.1 CGI_GDC.4.2 CGI_GDC.4.3 CGI_GDC.4.4 CGI_GDC.4.6 CGI_GIS.1.1 CGI_GIS.1.2 CGI_GIS.1.3

	CGI_GIS.1.4 CGI_GIS.1.5 CGI_GIS.1.6 CGI_GIS.1.7 CGI_GIS.1.8 CGI_LCI.1.1 CGI_LCI.1.2 CGI_LCI.1.3 CGS_GSS.2.1 CGS_GSS.2.2 CIS_SSI.1.1

ORG_25	
Coverage	BOS_SAT.1.3 BOS_SAT.2.1 CCS_CSP.1.1 CCS_CSP.1.2 CCS_CSP.1.3 CCS_CSP.1.4 CCS_CSP.2.1 CCS_SIN.1.1 CET_EGT.1.1 CET_EGT.1.2 CET_EGT.1.3 CET_EGT.1.4 CET_EGT.1.5 CET_EGT.1.6 CET_EGT.2.1 CET_EGT.2.2 CET_EGT.2.3 CET_EIP.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_PLD.1.4

ORG_26	
Coverage	BCM_RLC.1.1 BDM_ESS.1.1 BDM_SED.4.1 BDM_SED.5.1 BDM_SFS.1.1 BGC_PRS.2.1 CGS_PPS.2.3 CGS_PPS.2.4 CGS_REC.1.1

ORG_27	
Coverage	BGC_INT.2.1 BGC_PRS.2.1 BOS_SAT.1.2 BPE_SEM.1.1 BPE_SEM.3.1 BPE_SEM.3.2 BPE_SEM.4.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CCC_RGF.1.1 CCC_RGF.1.2 CET_EIP.1.3

	CET_EIP.1.6 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GMA.2.1 CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CGS_GSU.1.1 CGS_GSU.1.2 CGS_GSU.2.1 CGS_GSU.2.2 CGS_GSU.2.3 CGS_GSU.3.1 CGS_GSU.3.2 CGS_GSU.3.3 CGS_PDI.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_28	
Coverage	CDO_APP.1.1 CDO_APP.1.3 CGS_PPS.2.3
ORG_29	
Coverage	CPS_PAQ.1.1 CPS_PAQ.1.2 CPS_PAQ.1.3 CPS_PAQ.1.4 CPS_PAQ.1.5 CPS_PAQ.1.6
ORG_30	
Coverage	BCM_RLC.1.1 BCO_CEL.5.1 BDM_COC.2.1 BGC_GER.1.1 BGC_MSS.4.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAR.1.1 BMA_MAR.2.1 BMA_MAR.3.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.2.1 BOS_SAT.1.1 BOS_SAT.1.2 BOS_SAT.1.3 BOS_SAT.1.4 BOS_SAT.1.5 BOS_SAT.2.1 BPE_SEM.1.1 BPE_SEM.3.1 BPE_SEM.3.2

	BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CEI_ABS.1.1 CET_EGT.2.3 CGS_CSR.1.3 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.4 CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GMA.4.1 CGS_PAI.1.2 CGS_PAI.1.3 CGS_PDI.1.1 CGS_PEP.1.1 CGS_PPS.3.2 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_31	
Coverage	CEI_ABS.1.6 CEI_ABS.1.7 CRH_PDP.1.1
ORG_32	
Coverage	BPS_PSI.2.2 BPS_PSI.2.4 CEI_ABS.1.1 CEI_ABS.1.2 CEI_ABS.1.3 CEI_ABS.1.4 CEI_ABS.1.5
ORG_33	
Coverage	BCO_RPS.1.1 BCO_RPS.1.2 BDM_SSA.1.1 BDM_SSA.4.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1 BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.6.1 BMA_MAR.7.1 BMA_MAS.1.1 BMA_MAS.3.1 BMA_MAS.5.1 BMA_REU.2.1 BOS_SAT.1.2 BOS_SAT.1.5 BPE_SEM.1.1 BPE_SEM.3.1 BPE_SEM.3.2

	BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 BSP_SPR.3.1 CET_EGT.1.3 CET_PLD.1.2 CGS_GLI.2.1 CGS_OES.1.2 CGS_OES.1.3 CGS_PAI.2.1 CGS_PAI.2.2 CGS_PAI.2.3 CGS_PDI.1.1 CGS_PPS.2.5 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_34	
Coverage	BOS_ISI.5.1 BOS_ISI.5.2 BOS_ISI.5.3 BOS_ISI.6.1 BOS_ISI.6.2 BOS_ISI.6.3
ORG_35	
Coverage	BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1
ORG_36	
Coverage	CGS_GDH.1.3 CGS_PAI.1.4
ORG_37	
Coverage	BCO_CEL.1.1 BCO_CEL.4.1 BCO_CEL.7.1 BCO_CEL.7.2 BDM_SSA.1.1 BDM_SSA.4.1 BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BOS_SAT.1.3 BOS_SAT.2.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCC_CLR.1.1
ORG_38	
Coverage	BDM_SED.4.1 BDM_SED.5.1 BGC_PRE.6.1 BOS_ISI.4.1 BOS_ISI.7.1

	BOS_SOT.1.1 BOS_SOT.1.2 CCC_CLR.1.2 CGS_GPC.1.1 CGS_GPC.1.2 CGS_PPS.2.3 CRI_MOF.1.1 CRI_MOF.2.1
ORG_39	
Coverage	BDM_COC.2.1 BDM_COC.4.1 BGC_INT.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 CGS_GDA.1.4 FAU_SAA.2.1 FAU_SAA.2.2 FAU_SAA.2.3 FAU_SAA.3.1 FAU_SAA.3.2 FAU_SAA.3.3 FAU_STG.1/2.1 FAU_STG.1/2.2 FAU_STG.2.3 FAU_STG.3.1 FAU_STG.4.1
ORG_40	
Coverage	BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BPS_PSI.1.3
ORG_41	
Coverage	BGC_PRE.1.1 BMA_GAU.1.1 BPS_PSI.1.3 BSP_FOU.1.1 CDO_APP.1.1 CDO_APP.1.2
ORG_42	
Coverage	BDM_ESS.1.1 BDM_SFS.1.1 BGC_PRS.2.1 BMA_GAU.2.1 CGS_REC.1.1 FCO_NRO.1.1
ORG_43	
Coverage	CGS_GPC.2.1 CGS_GPC.2.2 CGS_GPC.2.3 CGS_GPC.2.4
ORG_44	
Coverage	CRR_ETU.1.1 CRR_ETU.1.2 CRR_ETU.2.2

Comments collection form

This form can be sent to the following address:

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
FRANCE
conseil.dcssi@sgdn.pm.gouv.fr

Contributor information
Name and organisation (optional): .....
E-mail address: .....
Date: .....

General remarks about the document
Does the document meet your needs? Yes ☐ No ☐

If yes:

Do you think its content could be improved? Yes ☐ No ☐

If yes:

What else would you like to have found in it?
.....
.....

Which sections of the document seem unhelpful or poorly adapted?
.....
.....

Do you think its form could be improved? Yes ☐ No ☐

If yes:

Which aspects could be improved?
- readability, comprehension ☐
- layout ☐
- other ☐

Specify the improvements in form you would like to see:
.....
.....

If no:

Specify the field for which it is poorly adapted and define what would have suited you:
.....
.....

Which other subjects would you like to see being dealt with?
.....
.....

Specific remarks about the document

Detailed comments can be formulated using the following table:

"No." indicates a sequential number.

"Type" comprises two letters:

The first letter indicates the remark category:

- O Spelling or grammar mistake
- E Lack of explanation or clarification for a given point
- I Incomplete or missing text
- R Error

The second letter indicates its seriousness:

- m minor
- M Major

"Reference" indicates the exact place in the text (paragraph number, line, etc.)

"Content of the remark" is where you should write the comment.

"Proposed solution" is used to submit a proposal for solving the problem described.

No.	Type	Reference	Content of the remark	Proposed solution
1				
2				
3				
4				
5				

Thank you for your help