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 4
TOOLS FOR ASSESSING ISS RISKS

Version 2 – 5 February 2004

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
05/02/2004	Publication of version 2 of the EBIOS guide	Validated

Table of contents

SECTION 1 – INTRODUCTION (separate document)

SECTION 2 – APPROACH (separate document)

SECTION 3 – TECHNIQUES (separate document)

SECTION 4 – TOOLS FOR ASSESSING ISS RISKS

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 fourth section of the method.

It includes :
- a classification of entity types and sub-types,
- a classification of attack methods, described according to the threat agents capable of using them,
- a vulnerability base arranged by attack method and listing all the types and sub-types concerned.

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

2 Entity types and sub-types

2.1 MAT : Hardware

MAT: Hardware	
Type	MAT: Hardware
Description	Description: ------------------- The hardware type consists of all the physical elements of an information system.

2.1.1 MAT_ACT : Data processing equipment (active)

MAT_ACT: Data processing equipment (active)	
Type	MAT_ACT: Data processing equipment (active)
Description	Description: ------------------- Automatic information processing equipment including the items it requires to operate independently. Affiliated entity types and sub-types: --- MAT: Hardware The hardware type consists of all the physical elements of an information system.
MAT_ACT.1: Transportable equipment	
Type	MAT_ACT.1: Transportable equipment
Description	Description: ------------------- Computer equipment designed to be carried by hand and used in different places. Examples: ------------------- Laptop computer, PDA. Affiliated entity types and sub-types: --- MAT: Harware The hardware type consists of all the physical elements of an information system.. MAT_ACT: Data processing equipment (active) Automatic information processing equipment including the items it requires to operate independently.
MAT_ACT.2: Fixed equipment	
Type	MAT_ACT.2: Fixed equipment
Description	Description: ------------------- Computer equipment belonging to the organisation or used in the organisation's premises. Examples: ------------------- Server, microcomputer used as a workstation. Affiliated entity types and sub-types: ---

	MAT: Hardware The hardware type consists of all the physical elements of an information system. MAT_ACT: Data processing equipment (active) Automatic information processing equipment including the items it requires to operate independently.

MAT_ACT.3: Processing peripheral	
Type	MAT_ACT.3: Processing peripheral
Description	Description: ------------------- Equipment connected to a computer via a communication port (serial, parallel link, etc.) for entering, conveying or transmitting data. Examples: ------------------- Printer, removable disc drive Affiliated entity types and sub-types: --- MAT: Hardware The hardware type consists of all the physical elements of an information system. MAT_ACT: Data processing equipment (active) Automatic information processing equipment including the items it requires to operate independently.

2.1.2 MAT_PAS : Data medium (passive)

MAT_PAS: Data medium (passive)	
Type	MAT_PAS: Data medium (passive)
Description	Description: ------------------- These are media for storing data or functions. Affiliated entity types and sub-types: --- MAT: Hardware The hardware type consists of all the physical elements of an information system.

MAT_PAS.1: Electronic medium	
Type	MAT_PAS.1: Electronic medium
Description	Description: ------------------- An information medium that can be connected to a computer or computer network for data storage. Despite their compact size, these media may contain a large amount of data. They can be used with standard computing equipment. Examples: ------------------- Floppy disc, CD ROM, back-up cartridge, removable hard disc, memory key, tape. Affiliated entity types and sub-types: --- MAT: Hardware The hardware type consists of all the physical elements of an information system. MAT_PAS: Data medium (passive) These are media for storing data or functions.

MAT_PAS.2: Other media	
Type	MAT_PAS.2: Other media

Description	Description: ------------------- Static, non-electronic media containing data. Examples: ------------------- Paper, slide, transparency, documentation, fax. Affiliated entity types and sub-types: -- MAT: Hardware The hardware type consists of all the physical elements of an information system. MAT_PAS: Data medium (passive) These are media for storing data or functions.

2.2 LOG: Software

LOG: Software	
Type	LOG: Software
Description	Description: ------------------- The software type consists of all the programmes contributing to the operation of a data processing set.

2.2.1 LOG_OS: Operating system

LOG_OS: Operating system	
Type	LOG_OS: Operating system
Description	Description : ------------------- This title includes all the programmes of a computer making up the operational base from which all the other programmes (services or applications) are run. It includes a kernel and basic functions or services. Depending on the architecture, an operating system may be monolithic or made up of a micro-kernel and a set of system services. The main components of the operating system are all the equipment management services (CPU, memory, discs, peripherals and network interfaces), task or process management services and user and user rights management services. Examples : ------------------- GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS. Affiliated entity types and sub-types: -- LOG : Software The software type consists of all the programmes contributing to the operation of a data processing set.

2.2.2 LOG_SRV: Service, maintenance or administration software

LOG_SRV: Service, maintenance or administration software	
Type	LOG_SRV: Service, maintenance or administration software
Description	Description : ------------------- Software characterised by the fact that it complements the operating system services and is not directly at the service of the users or applications (even though it is usually essential or even indispensable for the global operation of the information system). Examples : ------------------- GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS. Affiliated entity types and sub-types: -- LOG: Software The software type consists of all the programmes contributing to the operation of a data processing set.

2.2.3 LOG_STD: Package software or standard software

LOG_STD: Package software or standard software	
Type	LOG_STD: Package software or standard software
Description	Description : ------------------- Standard software or package software are complete products commercialised as such (rather than one-off or specific developments) with medium, release and maintenance. They provide "generic" services for users and applications, but are not personalised or specific in the way that business applications are. Examples: ------------------- Data base management software, electronic messaging software, groupware, directory software, Webserver software, etc. (Oracle, DB2, IIS, Apache, Lotus Notes, Exchange, OpenLDAP, etc.). Affiliated entity types and sub-types: -- LOG: Software The software type consists of all the programmes contributing to the operation of a data processing set.

2.2.4 LOG_APP : Business application

LOG_APP: Business application	
Type	LOG_APP: Business application
Description	Affiliated entity types and sub-types: -- LOG: Software The software type consists of all the programmes contributing to the operation of a data processing set.
LOG_APP.1: Standard business application	
Type	LOG_APP.1: Standard business application
Description	Description : ------------------- This is commercial software designed to give users direct access to the services and functions they require from their information system in their professional context. There is a very wide, theoretically limitless, range of fields. Examples: ------------------- Accounts software, machine tool control software, customer care software, personnel competency management software, administrative teleprocedure software, etc. Affiliated entity types and sub-types: -- LOG: Software The software type consists of all the programmes contributing to the operation of a data processing set. LOG_APP: Business application
LOG_APP.2: Specific business application	
Type	LOG_APP.2: Specific business application
Description	Description: ------------------- This is software in which various aspects (primarily support, maintenance, upgrading, etc.) have been specifically developed to give users direct access to

the services and functions they require from their information system in their professional context. There is a very wide, theoretically limitless, range of fields.

Examples:

Invoice management of telecom operators' customers, real time monitoring application for rocket launching

Affiliated entity types and sub-types:

LOG: Software
The software type consists of all the programmes contributing to the operation of a data processing set..
LOG_APP: Business application

2.3 RES : Network

RES: Network	
Type	RES: Network
Description	Description: ------------------- The network type consists of all telecommunications devices used to interconnect several physically remote computers or components of an information system.

2.3.1 RES_INF : Medium and supports

RES_INF: Medium and supports	
Type	RES_INF: Medium and supports
Description	Description: ------------------- Communications and telecommunications media or equipment are characterised mainly by the physical and technical characteristics of the equipment (point-to-point, broadcast) and by the communication protocols (link or network - levels 2 and 3 of the OSI 7-layer model). Examples: ------------------- PSTN, Ethernet, GigabitEthernet, cable, fibre, copper ADSL, WiFi 802.11, BlueTooth, FireWire. Affiliated entity types and sub-types: --- RES: Network The network type consists of all telecommunications devices used to interconnect several physically remote computers or components of an information system.

2.3.2 RES_REL : Passive or active relay

RES_REL: Passive or active relay	
Type	RES_REL: Passive or active relay
Description	Description: ------------------- This sub-type includes all devices that are not the logical terminations of communications (IS vision) but are intermediate or relay devices. These relays employ ad-hoc hardware, and often ad-hoc software. They are characterised by the supported network communication protocols. In addition to the basic relay, they often include routing and/or filtering functions and services, employing communication switches and routers with filters. They can often be administrated remotely and are sometimes capable of generating logs. Examples: ------------------- Bridge, router, hub, switch, automatic exchange. Affiliated entity types and sub-types: --- RES: Network The network type consists of all telecommunications devices used to interconnect several physically remote computers or components of an information system.

2.3.3 RES_INT : Communication interface

RES_INT: Communication interface	
Type	RES_INT: Communication interface
Description	Description: ------------------- The communication interfaces of the processing units. They are connected to the processing units, but are characterised by the media and supported protocols, by any installed filtering, log or warning generation functions and their capacities and by the possibility and requirement of remote administration. Examples: ------------------- Wifi, GPRS, Ethernet adaptor. Affiliated entity types and sub-types: -- RES: Network The network type consists of all telecommunications devices used to interconnect several physically remote computers or components of an information system.

2.4 PER : Personnel

PER: Personnel	
Type	PER: Personnel
Description	Description: ------------------- The personnel type consists of all the groups of persons involved in the information system.

2.4.1 PER_DEC : Decision maker

PER_DEC: Decision maker	
Type	PER_DEC: Decision maker
Description	Description: ------------------- Decision makers are the owners of the essential elements (information and functions) and the line managers of the organisation or specific project. Examples: ------------------- Top management, Project leader. Affiliated entity types and sub-types: --- PER: Personnel The personnel type consists of all the groups of persons involved in the information system.

2.4.2 PER_UTI : Users

PER_UTI: Users	
Type	PER_UTI: Users
Description	Description: ------------------- Users are the personnel who handle sensitive elements in the context of their activity and who have a special responsibility in this respect. They may have special access rights to the information system to carry out their everyday tasks. Examples: ------------------- Human resources management, Financial management, Risk manager. Affiliated entity types and sub-types: --- PER: Personnel The personnel type consists of all the groups of persons involved in the information system.

2.4.3 PER_EXP : Operator / Maintenance

PER_EXP: Operator / Maintenance	
Type	PER_EXP: Operator / Maintenance
Description	Description: ------------------- These are the personnel in change of operating and maintaining the information system. They have special access rights to the information system to carry out their everyday tasks.

	Examples: ------------------- System administrator, data administrator, back-up, Help Desk, application deployment operator, security officers. Affiliated entity types and sub-types: --- PER: Personnel The personnel type consists of all the groups of persons involved in the information system.

2.4.4 PER_DEV : Developer

PER_DEV: Developer	
Type	PER_DEV: Developer
Description	Description: ------------------- Developers are in charge of developing the organisation's applications. They have access to part of the information system with high-level rights but do not take any action on the production data. Examples: ------------------- Business application developers. Affiliated entity types and sub-types: --- PER: Personnel The personnel type consists of all the groups of persons involved in the information system.

2.5 PHY : Site

PHY: Site	
Type	PHY: Site
Description	Description: ------------------- The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate.

2.5.1 PHY_LIE : Places

PHY_LIE: Places	
Type	PHY_LIE: Places
Description	Description: ------------------- Perimeters, physical enclosures.

PHY_LIE.1: External environment	
Type	PHY_LIE.1: External environment
Description	Description: ------------------- This concerns all the places in which the organisation's means of security cannot be applied. Examples: ------------------- Homes of the personnel, premises of another organisation, environment outside the site (urban area, hazard area). Affiliated entity types and sub-types: --- PHY: Site The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate. PHY_LIE: Place Perimeters, physical enclosures.

PHY_LIE.2: Premises	
Type	PHY_LIE.2: Premises
Description	Description: ------------------- This place is bounded by the organisation's perimeter directly in contact with the outside. This may be a physical protective boundary obtained by creating physical barriers or means of surveillance around buildings. Examples: ------------------- Establishment, buildings. Affiliated entity types and sub-types: --- PHY: Site The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate. PHY_LIE: Place Perimeters, physical enclosures.

PHY_LIE.3: Zone

Type	PHY_LIE.3: Zone
Description	Description: ------------------- A zone is formed by a physical protective boundary forming partitions within the organisation's premises. It is obtained by creating physical barriers around the organisation's information processing infrastructures. Examples: ------------------- Offices, reserved access zone, secure zone. Affiliated entity types and sub-types: --- PHY: Site The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate. PHY_LIE: Place Perimeters, physical enclosures.

2.5.2 PHY_SRV : Essential service

PHY_SRV: Essential service	
Type	PHY_SRV: Essential service
Description	Description: ------------------- All the services required for the organisation's equipment to operate. Affiliated entity types and sub-types: --- PHY: Site The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate.

PHY_SRV.1: Communication	
Type	PHY_SRV.1: Communication
Description	Description: ------------------- Telecommunications services and equipment provided by an operator. Examples: ------------------- Telephone line, PABX, internal telephone networks. Affiliated entity types and sub-types: --- PHY: Site The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate. PHY_SRV: Essential service All the services required for the organisation's equipment to operate

PHY_SRV.2: Power	
Type	PHY_SRV.2: Power
Description	Description: ------------------- Services and means (sources and wiring) required for providing power to information technology equipment and peripherals. Examples: -------------------

	Low voltage power supply, inverter, electrical circuit head-end. Affiliated entity types and sub-types: --- PHY: Site The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate. PHY_SRV: Essential service All the services required for the organisation's equipment to operate.

PHY_SRV.3: Cooling / pollution

Type	PHY_SRV.3: Cooling / pollution
Description	Description: ------------------- Services and means (equipment, control) for cooling and purifying the air. Examples: ------------------- Chilled water pipes, air-conditioners. Affiliated entity types and sub-types: --- PHY: Site The site type comprises all the places containing the system, or part of the system, and the physical means required for it to operate. PHY_SRV: Essential service All the services required for the organisation's equipment to operate.

2.6 ORG : Organisation

ORG: Organisation	
Type	ORG: Organisation
Description	Description : ------------------- The organisation type describes the organisational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

2.6.1 ORG_DEP : Higher-tier organisation

ORG_DEP: Higher-tier organisation	
Type	ORG_DEP: Higher-tier organisation
Description	Description: ------------------- These are organisations on which the studied organisation depends. They may be legally affiliated or external. This imposes constraints on the studied organisation in terms of regulations, decisions, actions or reporting of information. Examples: ------------------- Administrating body, Head office of an organisation, Court of auditors. Affiliated entity types and sub-types: --- ORG The organisation type describes the organisational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

2.6.2 ORG_GEN : Structure of the organisation

ORG_GEN: Structure of the organisation	
Type	ORG_GEN: Structure of the organisation
Description	Description: ------------------- This consists of the various branches of the organisation, including its cross-functional activities, under the control of its management. Examples: ---------------- Human resources management, IT management, purchasing management, business unit management, building safety service, fire service, audit management. Affiliated entity types and sub-types: --- ORG The organisation type describes the organisational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

2.6.3 ORG_PRO : Project or system organisation

ORG_PRO: Project or system organisation	
Type	ORG_PRO: Project or system organisation

Description	Description: ------------------- This concerns the organisation set up for a specific project or service. Examples: ------------------- New application development project, information system migration project. Affiliated entity types and sub-types: --- ORG The organisation type describes the organisational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

2.6.4 ORG_EXT : Subcontractors / Suppliers / Manufacturers

ORG_EXT: Subcontractors / Suppliers / Manufacturers	
Type	ORG_EXT: Subcontractors / Suppliers / Manufacturers
Description	Description: ------------------- An organisation providing the organisation with a service or resources and bound to it by contract. Examples: ------------------- Facilities management company, outsourcing company, consultancy companies. Affiliated entity types and sub-types: --- ORG The organisation type describes the organisational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

2.7 SYS : System

SYS: System	
Type	SYS: System
Description	Description: ------------------- The system type consists of all specific facilities linked to information technologies, with a specific objective and operational environment. It is composed of various entities belonging to other types described above.

2.7.1 SYS_INT : Internet access device

SYS_INT: Internet access device	
Type	SYS_INT: Internet access device
Description	Description: ------------------- A device that dials the interconnection between the organisation's network and the Internet network and provides access services to or from the Internet. Examples: ------------------- Filtering device, DMZ, gateways. Affiliated entity types and sub-types: --- SYS: System The system type consists of all specific facilities linked to information technologies, with a specific objective and operational environment. It is composed of various entities belonging to other types described above.

2.7.2 SYS_MES : Electronic messaging

SYS_MES: Electronic messaging	
Type	SYS_MES: Electronic messaging
Description	Description: ------------------- A device allowing authorised users to type, query and send computerised documents or electronic messages from or to computers connected in network. Examples: ------------------- Internal electronic mail, Web electronic mail. Affiliated entity types and sub-types: --- SYS: System The system type consists of all specific facilities linked to information technologies, with a specific objective and operational environment. It is composed of various entities belonging to other types described above.

2.7.3 SYS_ITR : Intranet

SYS_ITR: Intranet	
Type	SYS_ITR: Intranet
Description	Description: ------------------- Shared and private data and information services, using communication protocols

	and core technologies (Internet technology for example). Examples: ------------------- Internal information system. Affiliated entity types and sub-types: --- SYS: System The system type consists of all specific facilities linked to information technologies, with a specific objective and operational environment. It is composed of various entities belonging to other types described above.

2.7.4 SYS_ANU : Company directory

SYS_ANU: Company directory	
Type	SYS_ANU: Company directory
Description	Description: ------------------- A device for managing and accessing a data base describing the company's personnel and their characteristics. Examples: ------------------- Management of application rights. Affiliated entity types and sub-types: --- SYS: Systeme The system type consists of all specific facilities linked to information technologies, with a specific objective and operational environment. It is composed of various entities belonging to other types described above.

2.7.5 SYS_WEB : External portal

SYS_WEB: External portal	
Type	SYS_WEB: External portal
Description	Description: ------------------- An external portal is a point of access that a user will find or use when he looks for information or a service provided by the organisation. Portals provide a wide range of resources and services. Examples: ------------------- Information portal, teleprocedure portal, electronic business site. Affiliated entity types and sub-types: --- SYS: System The system type consists of all specific facilities linked to information technologies, with a specific objective and operational environment. It is composed of various entities belonging to other types described above.

3 Generic attack methods and threat agents

The following table presents attack methods, showing the main ways in which they can violate security criteria. They are classified according to a representative theme (but may nonetheless be assigned to more than one theme).

Méthodes d'attaque	Availability	Confidentiality	Integrity
1 - Physical damage			
01 - FIRE	X		X
02 - WATER DAMAGE	X		X
03 - POLLUTION	X		X
04 - MAJOR ACCIDENT	X		X
05 - DESTRUCTION OF EQUIPMENT OR MEDIA	X		X
2 - Natural events			
06 - CLIMATIC PHENOMENON	X		X
07 - SEISMIC PHENOMENON	X		X
08 - VOLCANIC PHENOMENON	X		X
09 - METEOROLOGICAL PHENOMENON	X		X
10 - FLOOD	X		X
3 - Loss of essential services			
11 - FAILURE OF AIR-CONDITIONING	X		
12 - LOSS OF POWER SUPPLY	X		
13 - FAILURE OF TELECOMMUNICATION EQUIPMENT	X		
4 - Disturbance due to radiation			
14 - ELECTROMAGNETIC RADIATION	X		X
15 - THERMAL RADIATION	X		X
16 - ELECTROMAGNETIC PULSES	X		X
5 - Compromise of information			
17 - INTERCEPTION OF COMPROMISING INTERFERENCE SIGNALS		X	
18 - REMOTE SPYING	X	X	X
19 - EAVESDROPPING		X	
20 - THEFT OF MEDIA OR DOCUMENTS		X	
21 - THEFT OF EQUIPMENT	X	X	
22 - RETRIEVAL OF RECYCLED OR DISCARDED MEDIA		X	
23 - DISCLOSURE		X	
24 - DATA FROM UNTRUSTWORTHY SOURCES	X		X
25 - TAMPERING WITH HARDWARE		X	
26 - TAMPERING WITH SOFTWARE	X	X	X
27 - POSITION DETECTION		X	
6 - Technical failures			
28 - EQUIPMENT FAILURE	X		
29 - EQUIPMENT MALFUNCTION	X		
30 - SATURATION OF THE INFORMATION SYSTEM	X		
31 - SOFTWARE MALFUNCTION	X		X
32 - BREACH OF INFORMATION SYSTEM	X		

MAINTAINABILITY			
7 - Unauthorised actions			
33 - UNAUTHORISED USE OF EQUIPMENT	X	X	X
34 - FRAUDULENT COPYING OF SOFTWARE		X	
35 - USE OF COUNTERFEIT OR COPIED SOFTWARE	X		
36 - CORRUPTION OF DATA		X	X
37 - ILLEGAL PROCESSING OF DATA		X	
8 - Compromise of functions			
38 - ERROR IN USE	X	X	X
39 - ABUSE OF RIGHTS	X	X	X
40 - FORGING OF RIGHTS	X	X	X
41 - DENIAL OF ACTIONS			X
42 - BREACH OF PERSONNEL AVAILABILITY	X		

Attack methods are described according to the threat agents capable of using them.

Theme 1 – Physical damage

01 - FIRE

Description

Type

Natural / Human / Environmental

Accidental cause

Concentration of flammable or explosive materials in a confined environment, catching fire through an external event or internal accident.

Examples

Lightning, waste-paper bin fire, short circuit.

Deliberate cause

Terrorists or vandals gaining access to property in order to set light to flammable or explosive materials directly or indirectly (incendiary bombs, tampering with ventilation devices, etc.).

Examples

Striker gaining access to premises (through the IT room windows for example) to place an incendiary device in them.

Types of consequence

Destruction of assets.
Danger to personal safety.
Financial loss.
Disturbance of internal operation.

Severities

Integrity
Availability

02 - WATER DAMAGE

Description

Type

Natural / Human / Environmental.

Accidental cause

Flood due to a leak or burst pipe.

Examples

Leakage from air-conditioning equipment, leakage from a water room on the floor above, fire nozzle open.

Deliberate cause

Terrorists or vandals gaining access to the property to cause flooding in the rooms.

Examples

Deliberate breakage of pipes, triggering of extinguishing systems or simply spraying the equipment.

	Types of consequence ------------------------------------ Destruction or temporary unavailability of an asset. Financial loss. Disturbance of internal operation.
Severities	Integrity Availability
03 - POLLUTION	
Description	Type -------- Natural / Human / Environmental. Accidental cause ------------------------------ Presence of dust, vapours, corrosive or toxic gases in the ambient air. Examples ---------------- Exhaust gases in an area of heavy traffic. Deliberate cause -------------------------- Deliberate pollution of the ambient air by tampering with air-conditioning devices or placing a source of pollution in the rooms. Examples --------------- Malicious access and placing of pollutant in ventilation, heating or air-conditioning ducts. Types of consequence ------------------------------------ Destruction of an asset. Danger to personal safety. Availability of operational personnel.

Severities

Integrity
Availability

04 - MAJOR ACCIDENT

Description

Type

Natural / Environmental.

Accidental cause

External event or damage linked to the natural or industrial environment close to the assets and capable of causing them very serious physical damage.

Examples

Explosion of industrial sites in the vicinity, landslides, tidal wave, aircraft crashes, vehicle damaged or destroyed in a collision, etc.

Deliberate cause

External event or damage linked to an act of vandalism or terrorism close to the assets capable of causing them very serious physical damage.

Examples

Explosion of industrial sites in the vicinity, landslides, aircraft crashes, vehicle damaged or destroyed in a collision.

Types of consequence

Destruction of an asset.

Danger to personal safety.

Financial loss.

	Shutdown of operation.
Severities	Integrity Availability

05 - DESTRUCTION OF EQUIPMENT OR MEDIA

Description	Type -------- Human Accidental cause ------------------------------ Negligence or accidental event causing destruction of equipment or media. Examples --------------- Negligence during the transporting of equipment. Storage of archive media in an unsuitable environment. Damage caused by an animal. Spilling food or drink on equipment. Deliberate cause ------------------------- Person gaining access to equipment and causing its destruction. Examples --------------- Destruction of a machine and its back-ups (cartridge). Types of consequence ------------------------------------ Loss of data. Financial losses linked to the value of the equipment destroyed. Unavailability of the equipment.
Severities	Integrity Availability

Theme 2 – Natural events

06 - CLIMATIC PHENOMENON	
Description	Type -------- Natural Accidental cause ------------------------------- Specific climatic conditions (at operating limits of the equipment). Examples --------------- Site located in a geographical area prone to extreme heat, cold, humidity, wind or drought. Types of consequence ------------------------------------- Destruction or temporary shutdown of an asset.
Severities	Integrity Availability

07 - SEISMIC PHENOMENON	
Description	Type -------- Natural. Accidental cause ------------------------------- Earth tremor or earthquake causing extreme vibration or triggering a disaster (tidal wave). Examples ---------------

	Site housing an information system located in a geographical area subjected to frequent tremors. Types of consequence ------------------------------------ Destruction of an asset. Danger to personal safety.
Severities	Integrity Availability
08 - VOLCANIC PHENOMENON	
Description	Type -------- Natural. Accidental cause ------------------------------ Volcanic eruption causing vibrations or triggering another disaster (tidal wave). Examples --------------- Site housing an information system located in a geographical area known to be volcanic (intermittent phenomenon, active phases alternating with possibly very long dormant phases). Types of consequence ------------------------------------ Destruction of an asset. Danger to personal safety.
Severities	Integrity Availability
09 - METEOROLOGICAL PHENOMENON	
Description	Type --------

	Natural / Human. Accidental cause -------------------------------- Isolated atmospheric disturbance causing extreme climatic conditions Examples ---------------- Storms, hurricanes, cyclones, hail, lightning, avalanche. Deliberate cause -------------------------- A saboteur gains access to lightning protection devices. Examples --------------- Disconnection of the earthing system, short-circuiting of spark gaps, movement of the devices. Types of consequence ------------------------------------ Destruction of an asset. Danger to personal safety.
Severities	Integrity Availability
10 - FLOOD	
Description	Type -------- Natural. Accidental cause

	------------------------------ River, watercourse or underground water table causing periodic or exceptional flooding of land close by. Examples ---------------- The site may be located in a flood-prone area and be flooded by a river close by, or may be further away but subjected to the consequences of this flooding (landslide). Types of consequence ------------------------------------ Destruction of an asset. Danger to personal safety. Financial loss.
Severities	Integrity Availability

Theme 3 – Loss of essential services

11 - FAILURE OF AIR-CONDITIONING	
Description	Type -------- Human / Environmental. Accidental cause ------------------------------ Failure, shutdown or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction or fail completely. Examples --------------- Lack of maintenance for air-conditioning equipment, incorrect sizing of air-conditioning equipment, water supply cut off by the supplier. Deliberate cause -------------------------- A person can sabotage the equipment used to operate the air-conditioning system (cut off the water or power supply, destroy the system). Examples --------------- Shutdown of air-conditioning, water supply cut. Types of consequence ------------------------------------ Damage to assets. Availability
Severities	Availability
12 - LOSS OF POWER SUPPLY	
Description	Type

Human / Environmental.

Accidental cause

Failure, shutdown or incorrect sizing of the power supply to the assets arising either from the supplier's service or from the internal distribution system.

Examples

Interruption of the power company's service through strikes, breakdowns or work.

Fault or incorrect sizing of the internal power generator or emergency mains if these installations exist.

Connection of equipment with power rating in excessive of the emergency mains rating resulting in failure of the emergency equipment.

Lack of maintenance or ageing of the inverter batteries.

Accidental cutting of internal or external cables.

Interruption of water supply (by the supplier, or through internal error or negligence).

Deliberate cause

Sabotage or disturbance of the electrical installation by someone gaining access to the equipment (head-end, low voltage transformer, inverter, etc.)

Examples

Deliberate cutting of power provider's cables, deliberate shutting off of water supply.

Type of consequence

Temporary interruption of electricity supply or air-conditioning service.

Severities	Availability

13 - FAILURE OF TELECOMMUNICATION EQUIPMENT

Description	Type -------- Human / Environmental. Accidental cause ------------------------------ Disturbance, shutdown or incorrect sizing of telecommunications services (telephone, Internet access, Internet network). Examples --------------- Strikes, exceptional external event causing call saturation. Deliberate cause ------------------------- Sabotage or disturbance of the Telecom installation by someone gaining access to the telecommunications equipment (head-end, PABX, distribution frame, external cables, etc.) Examples --------------- Deliberate cutting of Telecom cables, destruction of an external exchange, deliberate saturation of the telecommunication passband. Type of consequence ------------------------------------ Slight or prolonged interruption of Telecommunication services. Financial loss.
Severities	Availability

Theme 4 – Disturbance due to radiation

14 - ELECTROMAGNETIC RADIATION

Description	Type -------- Human / Environmental. Accidental cause ------------------------------ Electromagnetic interference from an internal or external device. Examples ---------------- Radar, radio antenna, electricity generating station, machining tool. Deliberate cause ------------------------- Person using stray radiation to jam or saturate communications or disturb the operation of an appliance. Examples -------------- Jamming of WIFI communication. Type of consequence ------------------------------------ Distortion of cathode ray tube display, communication jamming. Modification or disturbance of operation.
Severities	Integrity Availability

15 - THERMAL RADIATION

Description	Type -------- Human / Natural / Environmental. Accidental cause ------------------------------ Thermal effect caused by a damage or exceptional weather conditions. Examples -------------- Forest fire creating conditions that exceed the operating characteristics of the equipment. Deliberate cause ------------------------- Device causing a thermal effect resulting in malfunction or destruction of equipment. Examples --------------- Placing of nuclear waste close to the information system, thermo-nuclear explosion. Type of consequence ------------------------------------ Malfunction or destruction of equipment. Danger to personal safety. Financial loss.

Severities

Integrity
Availability

16 - ELECTROMAGNETIC PULSES

Description

Type

Environmental.

Accidental cause

Damage causing an exceptional electromagnetic effect.

Examples

Industrial accident close to the site.

Deliberate cause

Electromagnetic pulses from nuclear sources.

Examples

Bombs.

Type of consequence

Destruction of property.
Financial loss.

Severities

Integrity
Availability

Theme 5 – Compromise of information

17 - INTERCEPTION OF COMPROMISING INTERFERENCE SIGNALS

Description	Type -------- Human. Deliberate cause ------------------------ Interfering signals from an electromagnetic source emitted by the equipment (by conduction on the electrical power supply cables or earth wires or by radiation in free space). Capture of these signals depends on the distance to the targeted equipment or the possibility of connecting to cables or any other conductor passing close to the equipment (coupling phenomenon). Examples ---------------- Spy or cracker intercepting or recording electromagnetic signals using sensors and electronic equipment on pipes. Spy or cracker intercepting and recording electromagnetic signals from radiation emitted by a video display terminal. Type of consequence ------------------------------------ Disclosure of communications or processing.
Severities	Confidentiality

18 - REMOTE SPYING

Description	Type -------- Human. Deliberate cause -------------------------- Personnel actions observable from a distance. Examples --------------- Visual observation with or without optical equipment, for example observation of a user entering a code or password on a keyboard. Type of consequence ----------------------------------- Intrusion. Misuse of identity.
Severities	Integrity Confidentiality Availability

19 - EAVESDROPPING

Description	Type -------- Human.

Deliberate cause

Someone connected to communication equipment or media or located inside the transmission coverage boundaries of a communication can use equipment, which may be very expensive, to listen to, save and analyse the information transmitted (voice or data).

Examples

Both radio and conducted signals can be intercepted. Sensors are used (for example an antenna for radio signals).

Infrared communications may also be intercepted.

For wire communications, a device already connected to the network (such as a workstation in a local network) can be used to store and analyse transmitted information (such as information exchanged with a server). Many commercial products are available to assist analysis and interpret frames in any communication protocol in real time..

Type of consequence

Disclosure of information transmitted on a communication medium.

Severities

Confidentiality

20 - THEFT OF MEDIA OR DOCUMENTS

Description

Type

Human.

Deliberate cause

Someone inside or outside the organisation accessing digital media or paper documents with the intention of stealing and using the information on them.

Examples

Theft of floppy discs, CD-ROMs, cartridges, back-up tapes.
Theft of files, notes, drawings, reports.
Theft of printouts left temporarily on printers in shared rooms.
Searching in waste paper bins left on public ways.

Type of consequence

Disclosure of information (assets, passwords).

Severities

Confidentiality

21 - THEFT OF EQUIPMENT

Description	Type -------- Human. Deliberate cause -------------------------- Someone inside or outside the organisation accessing equipment located on the premises or transported outside, out of greed or for strategic reasons. Examples ---------------- Theft of a laptop computer to sell it, theft of a PDA to make use of its contents. Type of consequence ------------------------------------ Loss of information and/or functions (for example portable equipment used for maintenance). Disclosure of the information stored on the equipment (for example passwords, extracts from information assets). Financial loss.
Severities	Confidentiality Availability

22 - RETRIEVAL OF RECYCLED OR DISCARDED MEDIA

Description	Type -------- Human. Accidental cause ------------------------------ Retrieval of electronic media (hard discs, floppy discs, back-up cartridges, USB keys, ZIP discs, removable hard discs, etc.) or paper copies (lists, incomplete print-outs, messages, etc.) intended for recycling and containing retrievable information. Example -------------- Recycling of computers whose hard discs have not been formatted, for use by other users in the same organisation, schools, other organisations.Reuse of paper for rough copies in the same organisation or outside. Deliberate cause -------------------------- Retrieval of electronic media (hard discs, floppy discs, back-up cartridges, USB

keys, ZIP discs, removable hard discs, etc.) or paper copies (lists, incomplete print-outs, messages, etc.) intended for destruction and containing retrievable information.

Example

Searching in waste paper bins left on public ways.

Type of consequence

Loss of customer confidence.
Disclosure of information.

Severities

Confidentiality

23 - DISCLOSURE

Description

Type

Human.
Accidental cause

Someone inside the organisation who, through negligence, passes information to others in the organisation who have no need to know or to the outside (the latter case usually having greater consequences).
Examples

Message sent to the wrong recipient.
Response to enquiries without checking the source (malicious request for passwords).
Unfamiliarity with the information distribution rules applied in the organisation.
Oversight committed in the definition of the rules controlling access to shared information.
Failure to comply with basic rules of discretion (discussion or reading a document in public places).

Deliberate cause

Someone knowingly passing on information inside the organisation to others who have no need to know or to the outside (the latter case usually having greater consequences).

Examples

Someone passing on confidential information by electronic messaging out of revenge.
Someone disclosing information under the belief that being in possession of sensitive information gives him/her a certain power over others.
Passing on information to a third party under the pressure of blackmail.Using industrial or commercial information for financial gain (industrial espionage).

Type of consequence

Attack on users' private life.
Disclosure of information assets.
Financial loss.

Severities

Confidentiality

24 - DATA FROM UNTRUSTWORTHY SOURCES

Description

Type

Human.

	Accidental cause ------------------------------ Receiving false data or unsuitable equipment from outside sources and using them in the organisation. Examples --------------- Information from a discussion forum. Downloading updates from Internet sites that do not belong to the developer concerned. Information received without sender identification or authentication, for example receiving electronic mail transmitted by a generic company identification (support@société.com). Deliberate cause ------------------------- Someone transmitting false information for integration in the information system with the intention of misinforming the recipient and attacking the reliability of the system or validity of its information. Examples --------------- Transmitting hoaxes by electronic messaging. Someone transmitting data and pretending to be the legitimate source. Type of consequence ------------------------------------ Corruption of data or processing. Wasted use of human resources. Loss of customer confidence.
Severities	Integrity Availability
25 - TAMPERING WITH HARDWARE	
Description	Type -------- Human. Deliberate cause ------------------------- Someone with access to a communication medium or equipment installs an interception or destruction device in it. Examples ---------------- Inserting a PCB in a micro-computer during its transport. Setting up a microphone in equipment.Tapping voice or data communication circuits. Trapping a function of a protection device to disable it and then commit an attack. Type of consequence ------------------------------------ Disclosure of information outside the organisation. Destruction of a device during a critical period. Disabled protection function.
Severities	Confidentiality
26 - TAMPERING WITH SOFTWARE	
Description	Type -------- Human / Environmental.

Accidental cause

Unintentional action involving software carried out from inside or outside the organisation and resulting in corruption or destruction of programmes or data, impaired operation of the resource or even execution of commands in a user's name without his/her knowledge.

Examples

User connecting a laptop computer to a network infected by a virus, introduced during an exchange with a different organisation.
An information system user receiving a worm from a source outside the organisation and unknowingly spreading it inside the organisation.

Deliberate cause

The attacker introduces a programme or commands in order to modify the behaviour of a programme or add an unauthorised service to an operating system.
This threat agent may act on the information system during the design, pre-production, production, operating, transport or maintenance phase.

Examples

Having a user run a programme by simulating an action that is authorised but contains hidden functions capable of infringing the security policy (Trojan horse).
A logic bomb added to a programme by the programmer to insert a command, generally with a triggering condition (date, contextual event), which runs an unauthorised action.

Types of consequence

Intrusion.
Disturbance of operation.
Destruction of data.
Corruption of the software.

Severities

Integrity
Confidentiality
Availability

27 - POSITION DETECTION

Description

Type

Human.

Deliberate cause

Someone with access to equipment used to detect the position of an information system user.

Examples

Access to entry/exit records.Access to ticket requests.
Use of antennas to which mobile phones are connected during operation in order to detect a person's position.

Types of consequence

Use of information to carry out targeted attacks.

Severities

Confidentiality

Theme 6 – Technical failures

28 - EQUIPMENT FAILURE	
Description	Type -------- Human / Natural. Accidental cause ------------------------------ Event causing equipment failure. Examples --------------- Wear, ageing, lack of maintenance or incorrect use (for example, incorrect sizing, use outside the operating limits) causing a failure. Types of consequence ------------------------------------ Unavailability of an equipment item. Corruption or loss of information.
Severities	Availability

29 - EQUIPMENT MALFUNCTION	
Description	Type -------- Human / Natural. Accidental cause ------------------------------ A logical or physical event causing an equipment item to malfunction. Examples --------------- Failure to follow equipment qualification procedures after updates or upgrades.Unintentional damage to an equipment item. Use of equipment under conditions outside its operating limits (temperature, humidity). Wear or ageing of equipment. Types of consequence ------------------------------------ Interrupted operation of a device which, through a side effect, may result in unavailability of the information system.
Severities	Availability

30 - SATURATION OF THE INFORMATION SYSTEM	
Description	Type -------- Human. Accidental cause ------------------------------ Hardware, software or network resource inadequate for meeting users' needs. Examples -------------- Overload of storage space (e.g. back-up space, mailbox storage, work area, etc.) for example, saturation of a mailbox when its owner is absent for long periods. Saturation due to overworking the machine (too many requests processed

	simultaneously). Equipment incorrectly sized (inverters, communication channels, etc.) Deliberate cause -------------------------- An attacker simulates an intense demand on resources by setting up continuous bombardment. Examples ---------------- Running a very large number of simultaneous commands. Deliberate saturation of space used for storing system or application activity tracks in order to hide unauthorised operations. Types of consequence ------------------------------------ Shutdown causing temporary unavailability of the service. Loss of information.
Severities	Availability

31 - SOFTWARE MALFUNCTION

Description	Type -------- Human / Environmental. Accidental cause ------------------------------ Design error, installation error or operating error committed during modification causing incorrect execution. Examples ---------------- Implementation error resulting in incorrect processing of data at terminals.Installation of software causing side effects. Failure to comply with installation or operation procedures. Error committed during maintenance operations. Types of consequence ------------------------------------ Interruption of service. Incorrect operation. Production of corrupted data.
Severities	Integrity Availability

32 - BREACH OF INFORMATION SYSTEM MAINTAINABILITY

Description	Type -------- Human / Environmental. Accidental cause ------------------------------ Lack of expertise in the system making retrofitting and upgrading impossible; for example, inability to correct an operating problem or respond to new needs. Examples ---------------- Failure of hardware and software suppliers. Failure of external software and hardware maintenance companies, termination of support contract leaving a lack of competency or resources for system upgrading.

	A system modified so many times that it has become difficult, or even impossible, to maintain without the risk of side effects after modification. Deliberate cause ------------------------- Someone making the system difficult, or even impossible, to upgrade. Examples ---------------- Out of spite, a person leaves no records or help for maintaining the system (rendering it opaque). Types of consequence ------------------------------------ Prolonged interruption of service. Breach of operating security. Financial losses resulting from replacing equipment or changing supplier.
Severities	Availability

Theme 7 – Unauthorised actions

33 - UNAUTHORISED USE OF EQUIPMENT

Description

Type

Human.

Deliberate cause

A person inside or outside the organisation accesses the information system and uses one of its services to penetrate it, run operations or steal information.

Examples

Theft of authorised user identification/authentication data in order to acquire user rights and bypass access checks, access to protected areas from an authorised access using a flaw in the application mechanisms to bypass the protection system.
Reading and looking up information from residual data on electronic media (cache memory file, snippets of residual information on hard discs, context back-ups - restore points used to undo problems - containing system status information that can be looked up by a well-informed attacker).
Simulation of machine behaviour to deceive an authorised user and acquire his/her name and password.
Deliberate modification or destruction of data.

Types of consequence

Intrusion into the information system.
Disclosure of information.

Severities

Integrity
Confidentiality
Availability

34 - FRAUDULENT COPYING OF SOFTWARE

Description

Type

Human.

Deliberate cause

Someone inside the organisation makes fraudulent copies (also called pirated copies) of package software or in-house software.

Examples

Copying the organisation's software for fun, out of revenge (broadcasting via Internet) or out of greed (sale).

Types of consequence

Financial loss.
Loss of customer confidence.

Severities

Confidentiality

35 - USE OF COUNTERFEIT OR COPIED SOFTWARE

Description

Type

Human / Environmental.

Accidental cause

Loss or destruction of documents proving the purchase of licences or negligence committed by installing software without paying for the licence.

Examples

Proof of purchase accidentally destroyed.Inability to produce a licence inventory.

Deliberate cause

Someone inside the organisation makes illegal use of copied software.

Examples

Software copied without licence to carry out an authorised task in the organisation.

Types of consequence

Breach of the law.
Loss of customer confidence.

Severities

Availability

36 - CORRUPTION OF DATA

Description

Type

Human.

Deliberate cause

Someone gains access to the communication equipment of the information system and corrupts transmission of information (by intercepting, inserting, destroying, etc.) or repeatedly attempts access until successful.

Examples

Destroying, inserting or modifying messages (modifying information, rearranging information within messages or rearranging the order of messages).
Denial of service (delaying a message).
IP address sweep from outside the organisation until an address giving access to the information system is found.

Types of consequence

Intrusion.
Corruption of communications.

Severities

Integrity
Confidentiality

37 - ILLEGAL PROCESSING OF DATA

Description

Type

Human.

Deliberate cause

A person carries out information processing that is forbidden by the law or a regulation.

	Examples ---------------- Creating and using an undeclared personal data file (illegal use of records). Carrying out forbidden operations on declared personal data files such as comparing several files. Encrypting data for reasons of confidentiality using long keys without prior authorisation.Illegal use of data from a recycled computer. Types of consequence ------------------------------------- Attack on users' private life. Judicial proceedings and penalties.
Severities	Confidentiality

Theme 8 – Compromise of functions

38 - ERROR IN USE

Description

Type

Human.

Accidental cause

A person commits an operating error, input error or utilisation error on hardware or software.

Examples

Loss of data following an error during back-up operations.
Failure to comply with installation or maintenance procedures.
Error by console operator entering a large amount of data containing figures.
Negligence committed when setting the parameters of a protection programme.
Recipient's address entered incorrectly on an e-mail.

Types of consequence

Interruption of service.
Corruption of data.
Malfunction, loss of effectiveness of protection means, introduction of additional flaws.
Unintentional disclosure of data.

Severities

Integrity
Confidentiality
Availability

39 - ABUSE OF RIGHTS

Description

Type

Human.

Accidental cause

Someone with special rights (network administration, computer specialists, etc.) modifies the operating characteristics of the resources without informing the users.

Examples

New access rights are created without taking into account the needs for protecting data stored by the users.
Back-up procedure stopped without users being informed.
Configuration parameters modified on servers causing side effect and malfunctions.

Deliberate cause

Someone accesses the system to modify, delete or add operating characteristics or carry out any other unauthorised operation possible to holders of these rights.

Examples

An administrator changes users' passwords.
A maintenance agent modifies the behaviour of the security mechanisms to access protected information.

	The event log is deleted on the application servers. Types of consequence ------------------------------------ Impaired operation. Disclosure of information. Loss of information.
Severities	Integrity Confidentiality Availability

40 - FORGING OF RIGHTS

Description	Type -------- Human. Deliberate cause ------------------------- A person assumes the identity of a different person in order to use his/her access rights to the information system, misinform the recipient, commit a fraud, etc. Examples ---------------- A person assumes the identity of a user and, claiming to have lost a password, requests the administrator to cover his/her access. A person takes over a session left open by its authorised user. Types of consequence ------------------------------------ Intrusion.
Severities	Integrity Confidentiality Availability

41 - DENIAL OF ACTIONS

Description	Type -------- Human. Deliberate cause ------------------------- A person or entity denies being involved in an exchange with a third party or carrying out an operation. Examples ---------------- Someone denying that he/she has received or sent a given message or claiming to have sent (received) a different message (file) or claiming not to have carried out an operation. Types of consequence ------------------------------------ Absence of proof.
Severities	Integrity

42 - BREACH OF PERSONNEL AVAILABILITY

Description	Type ------- Human / Environmental.

	Accidental cause ------------------------------ Absence of qualified or authorised personnel held up for reasons beyond their control. Examples ---------------- Illness, death, transport strike. Deliberate cause -------------------------- Deliberate absence of qualified or authorised personnel. Examples -------------- Strikes, leave not approved by the organisation. Types of consequence ------------------------------------ Stoppage, service disturbance.
Severities	Availability

4 Generic vulnerabilities

Vulnerabilities are arranged by attack method and indicate the types and sub-types concerned. Entity sub-types inherit the vulnerabilities of their entity type.

4.1 FIRE

Single copy of licence contracts	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP.1: Standard business application
Single internally-developed applications	
Types of entity	LOG_STD: Package software or standard software LOG_APP.2: Specific business application
No substitution equipment	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Equipment using flammable materials (e.g. bulk printers producing dust)	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No back-up of data contained on the media	
Types of entity	MAT_PAS.1: Electronic medium
Original media	
Types of entity	MAT_PAS.2: Other media
No insurance cover for serious damage	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation
No site inspection by emergency services (fire-fighting services)	
Types of entity	ORG_DEP: Higher-tier organisation
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses guaranteeing cover of the activities if a crisis is declared at the supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No security instructions given to external personnel working on the premises	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No management of emergency equipment inspection reports	
Types of entity	ORG_GEN: Structure of the organisation

No updated display of information for calling the emergency services	
Types of entity	ORG_GEN: Structure of the organisation
No fire-fighting organisation (description of roles and responsibilities)	
Types of entity	ORG_GEN: Structure of the organisation
No monitoring of maintenance contracts for fire-fighting equipment	
Types of entity	ORG_GEN: Structure of the organisation
No crisis management organisation	
Types of entity	ORG_PRO: Project or system organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No test of reaction and information procedures in the event of an accident	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No awareness programme for protection of security equipment	
Types of entity	PER_DEC: Decision maker
Conflictual industrial relations	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Presence of an opening onto a public right-of-way (window)	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone PHY_LIE.2: Premises
Ageing of the premises	
Types of entity	PHY_LIE.2: Premises
No control of access to the site or premises	
Types of entity	PHY_LIE.2: Premises
No fire partitions	
Types of entity	PHY_LIE.2: Premises
No precautions taken at the installation phase for fire risks specific to the equipment housed.	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone
No sizing of the automatic fire extinction system, or incorrect sizing or inadequacy of	

this system.	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone
No maintenance of air-conditioning equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
VULNERABILITIES LINKED TO ATTACK METHOD 01 - FIRE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.2 WATER DAMAGE

Single copy of licence contracts	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP.1: Standard business application
Single internally-developed applications	
Types of entity	LOG_STD: Package software or standard software LOG_APP.2: Specific business application
No substitution equipment	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No back-up of data contained on the media	
Types of entity	MAT_PAS.1: Electronic medium
Original media	
Types of entity	MAT_PAS.2: Other media
No insurance cover for serious damage	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No security instructions given to external personnel working on the premises	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No management of emergency equipment inspection reports	
Types of entity	ORG_GEN: Structure of the organisation
No updated display of information for calling the emergency services	
Types of entity	ORG_GEN: Structure of the organisation
No warning, reaction or information instructions in the event of water damage (no identification of stop cocks, etc.)	
Types of entity	ORG_GEN: Structure of the organisation
No guarantee that water detectors are operating correctly	
Types of entity	ORG_GEN: Structure of the organisation
No crisis management organisation	
Types of entity	ORG_PRO: Project or system organisation
No test of reaction and information procedures in the event of an accident	

Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No awareness programme for protection of security equipment	
Types of entity	PER_DEC: Decision maker
Conflictual industrial relations	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Site located in flood-prone area	
Types of entity	PHY_LIE.1: External environment
No control of physical access points to the premises	
Types of entity	PHY_LIE.2: Premises
External opening not watertight	
Types of entity	PHY_LIE.2: Premises
Presence of a fire extinction system using water	
Types of entity	PHY_LIE.2: Premises
Ceiling or external opening not watertight	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone
No clear identification of water stop cocks	
Types of entity	PHY_LIE.3: Zone
Unprotected access point	
Types of entity	PHY_LIE.3: Zone
Water pipe close to equipment	
Types of entity	PHY_LIE.3: Zone
Fire extinction system using water	
Types of entity	PHY_LIE.3: Zone
Water pipe close to termination equipment	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone
No sump	
Types of entity	PHY_LIE.3: Zone

Unprotected access to rooms housing production equipment or distribution equipment for essential services	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication
Wiring laid on the floor	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication
Ageing of cooling pipes	
Types of entity	PHY_SRV.3: Cooling / pollution
No maintenance of air-conditioning equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
No water stop cock	
Types of entity	PHY_SRV.3: Cooling / pollution
VULNERABILITIES LINKED TO ATTACK METHOD 02 - WATER DAMAGE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment

	MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.3 POLLUTION

Single copy of licence contracts	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP.1: Standard business application
Single internally-developed applications	
Types of entity	LOG_STD: Package software or standard software LOG_APP.2: Specific business application
Medium sensitive to storage conditions	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No monitoring of maintenance contracts	
Types of entity	ORG_GEN: Structure of the organisation
No measures in the event of interruption of air-conditioning service	
Types of entity	ORG_GEN: Structure of the organisation
No test of reaction and information procedures in the event of an accident	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No awareness programme for protection of security equipment	
Types of entity	PER_DEC: Decision maker
Conflictual industrial relations	
Types of entity	PER_UTI: Users

	PER_EXP: Operator / Maintenance PER_DEV: Developer
Proximity of pollution sources (noise, smoke, vapour, etc.)	
Types of entity	PHY_LIE.2: Premises PHY_LIE.1: External environment
Polluted atmosphere (hangar, workshop, etc.)	
Types of entity	PHY_LIE.2: Premises
No maintenance of air-conditioning equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
No correctly sized redundant equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
Ageing of air-conditioning filters	
Types of entity	PHY_SRV.3: Cooling / pollution
Unprotected access to equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
VULNERABILITIES LINKED TO ATTACK METHOD 03 - POLLUTION	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium

	MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.4 MAJOR ACCIDENT

Single copy of licence contracts	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP.1: Standard business application
Single internally-developed applications	
Types of entity	LOG_STD: Package software or standard software LOG_APP.2: Specific business application
No substitution equipment	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No back-up of data contained on the media	
Types of entity	MAT_PAS.1: Electronic medium
Original media	
Types of entity	MAT_PAS.2: Other media
No emergency service close to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No updated display of information for calling the emergency services	
Types of entity	ORG_GEN: Structure of the organisation
No insurance cover for serious damage	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No crisis management organisation	
Types of entity	ORG_PRO: Project or system organisation

	ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No emergency situation management procedures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance
Possibilities of destruction caused by an external event (collisions, attacks)	
Types of entity	PHY_LIE.1: External environment
Proximity of industrial activity or potentially hazardous site	
Types of entity	PHY_LIE.1: External environment
Rooms in which explosion/implosion risks have not been taken into account	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone PHY_LIE.2: Premises
VULNERABILITIES LINKED TO ATTACK METHOD 04 - MAJOR ACCIDENT	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers

	ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.5 DESTRUCTION OF EQUIPMENT OR MEDIA

Single copy of licence contracts	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP.1: Standard business application
Single internally-developed applications	
Types of entity	LOG_STD: Package software or standard software LOG_APP.2: Specific business application
No substitution equipment	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Fragility of equipment	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Equipment accessible to persons other than its owners (e.g. located in a passage way)	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Medium accessible to persons other than its owners	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No archiving procedure	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media

	MAT_PAS.1: Electronic medium
Fragility of media	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No archive storage measures suitable for the storage periods (ageing of tapes, wear of CD-ROMs)	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No back-up of data contained on the media	
Types of entity	MAT_PAS.1: Electronic medium
Original media	
Types of entity	MAT_PAS.2: Other media
No instructions given to external personnel working on the premises	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No insurance cover for destruction of equipment	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No rules for the use and storage of hardware and information media (protection conditions during transport, smoking ban, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Conflictual industrial relations	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Inadequate awareness programme concerning physical protection of equipment	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
No control of access to the site or premises or possibility of intrusion via indirect access routes.	
Types of entity	PHY_LIE.2: Premises PHY_LIE.1: External environment
Unprotected physical access to rooms housing equipment or media.	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution

	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone
Media accessible to unauthorised persons	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
Unidentified underground equipment	
Types of entity	RES_INF: Medium and supports
Equipment accessible to unauthorised persons	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Fragility of equipment	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
VULNERABILITIES LINKED TO ATTACK METHOD 05 - DESTRUCTION OF EQUIPMENT OR MEDIA	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium

	MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.6 CLIMATIC PHENOMENON

Conditions of use outside operating limits of the equipment	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No emergency service close to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No test of reaction and information procedures in the event of an accident	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
No means of ventilation or air-conditioning during excessive summer heat	
Types of entity	PHY_LIE.3: Zone

	PHY_LIE.2: Premises
Climatic conditions not taken into account in the construction of the premises	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
VULNERABILITIES LINKED TO ATTACK METHOD 06 - CLIMATIC PHENOMENON	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system

	LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.7 SEISMIC PHENOMENON

Equipment sensitive to vibrations	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No emergency service close to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No test of reaction and information procedures in the event of an accident	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Seismic conditions not taken into account in the construction of the buildings	
Types of entity	PHY_LIE.2: Premises
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
VULNERABILITIES LINKED TO ATTACK METHOD 07 - SEISMIC PHENOMENON	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory

	SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.8 VOLCANIC PHENOMENON

No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No emergency service close to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation

	ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No test of reaction and information procedures in the event of an accident	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Site listed as volcano-prone	
Types of entity	PHY_LIE.1: External environment
Seismic conditions not taken into account in the construction of the buildings	
Types of entity	PHY_LIE.2: Premises
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
VULNERABILITIES LINKED TO ATTACK METHOD 08 - VOLCANIC PHENOMENON	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation

	ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.9 METEOROLOGICAL PHENOMENON

Conditions of use outside operating limits of the equipment	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
No emergency service close to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No test of reaction and information procedures in the event of an accident	

Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Site in which extreme weather phenomena occur periodically (storm, hurricane, cyclone, etc.)	
Types of entity	PHY_LIE.1: External environment
No protection against lightning	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
VULNERABILITIES LINKED TO ATTACK METHOD 09 - METEOROLOGICAL PHENOMENON	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium

	MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.10 FLOOD

No emergency service close to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering a crisis declared at a subcontractor's or supplier's site	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Site located in flood-prone area	
Types of entity	PHY_LIE.1: External environment
No protection against rising water levels	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE.3: Zone PHY_LIE.2: Premises
Medium or equipment not designed to resist extreme conditions (of humidity, temperature or physical disturbances).	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
VULNERABILITIES LINKED TO ATTACK METHOD 10 - FLOOD	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System

	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.11 FAILURE OF AIR-CONDITIONING

Equipment requiring air-conditioning in order to operate	
Types of entity	MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment
Archives requiring air-conditioning for their preservation	
Types of entity	MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering compensation for damage in the event of loss of an essential service	

Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No contractual clauses covering the maximum acceptable downtime of an essential service	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No revision of air-conditioning needs when premises are modified or equipment is added.	
Types of entity	PHY_LIE.3: Zone
System depending on a chilled water or power supplier	
Types of entity	PHY_SRV.3: Cooling / pollution
System not adequately sized to meet the needs	
Types of entity	PHY_SRV.3: Cooling / pollution
No maintenance of air-conditioning equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
No correctly sized redundant equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
Unprotected access to water and power supply equipment	
Types of entity	PHY_SRV.3: Cooling / pollution
VULNERABILITIES LINKED TO ATTACK METHOD 11 - FAILURE OF AIR-CONDITIONING	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises

	PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.12 LOSS OF POWER SUPPLY

Equipment sensitive to electrical disturbances (voltage drops, overvoltages, transient power-cuts)	
Types of entity	RES_REL: Passive or active relay MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering compensation for damage in the event of loss of an essential service	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No contractual clauses covering the maximum acceptable downtime of an essential service	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users

	PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Lack of information concerning conditions of use of emergency power supply points	
Types of entity	PER_UTI: Users
Terminal communication equipment with no emergency power supply	
Types of entity	PHY_SRV.1: Communication
Rooms containing acid-based batteries are not specifically designed and physically isolated from the equipment to which they are connected	
Types of entity	PHY_SRV.2: Power
Incorrect sizing of emergency power supply equipment (inverter, batteries, etc.)	
Types of entity	PHY_SRV.2: Power
Unprotected physical access to rooms housing electrical power supply and distribution equipment	
Types of entity	PHY_SRV.2: Power
Rooms containing acid-based batteries are not fitted with mechanical ventilation and explosion-proof electrical equipment.	
Types of entity	PHY_SRV.2: Power
The floor or wall coverings are not anti-static	
Types of entity	PHY_SRV.2: Power
The low voltage panel is not accessible	
Types of entity	PHY_SRV.2: Power
The medium / low voltage transformer substation is not installed on the site (with controlled supplier access)	
Types of entity	PHY_SRV.2: Power
No analysis of emergency power level required if equipment is added	
Types of entity	PHY_SRV.2: Power
Earthing of exposed conductive parts does not comply with regulations	
Types of entity	PHY_SRV.2: Power
VULNERABILITIES LINKED TO ATTACK METHOD 12 - LOSS OF POWER SUPPLY	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution

	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.13 FAILURE OF TELECOMMUNICATION EQUIPMENT

Equipment maintained remotely via telecommunication equipment	
Types of entity	RES_REL: Passive or active relay MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No installation standard for sites belonging to the organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering compensation for damage in the event of loss of an essential service	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No contractual clauses covering the maximum acceptable downtime of an essential service	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions (warning, prevention, reaction, etc.)	
Types of entity	ORG_PRO: Project or system organisation

	ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No maintenance of termination and distribution equipment	
Types of entity	PHY_SRV.1: Communication
Operating faults on the internal telephone network	
Types of entity	PHY_SRV.1: Communication
Operating problem already encountered on the telecommunication service supply	
Types of entity	PHY_SRV.1: Communication
Unprotected physical access to rooms housing electrical power supply and distribution equipment or telecommunication equipment	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication
VULNERABILITIES LINKED TO ATTACK METHOD 13 - FAILURE OF TELECOMMUNICATION EQUIPMENT	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive)

	MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.14 ELECTROMAGNETIC RADIATION

Equipment or medium sensitive to electromagnetic or thermal radiation	
Types of entity	MAT_ACT.2: Fixed equipment
No contractual clause relating to electromagnetic compatibility	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
Risk of electromagnetic or thermal radiation not taken into account in the design	
Types of entity	PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment
Proximity of a source of electromagnetic or thermal radiation	
Types of entity	PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment
Risks arising from the proximity of an electromagnetic source not taken into account	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication
Medium and supports sensitive to electromagnetic or thermal radiation	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
VULNERABILITIES LINKED TO ATTACK METHOD 14 - ELECTROMAGNETIC RADIATION	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay

	RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.15 THERMAL RADIATION

Equipment or medium sensitive to electromagnetic or thermal radiation	
Types of entity	MAT_ACT.2: Fixed equipment

Proximity of a source of electromagnetic or thermal radiation	
Types of entity	PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment

Risk of electromagnetic or thermal radiation not taken into account in the design	
Types of entity	PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises

	PHY_LIE.1: External environment
Risks arising from the proximity of an electromagnetic source not taken into account	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication
Medium and supports sensitive to electromagnetic or thermal radiation	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
VULNERABILITIES LINKED TO ATTACK METHOD 15 - THERMAL RADIATION	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application

	LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.16 ELECTROMAGNETIC PULSES

Equipment or medium sensitive to electromagnetic or thermal radiation	
Types of entity	MAT_ACT.2: Fixed equipment
Proximity of a source of electromagnetic or thermal radiation	
Types of entity	PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment
Risk of electromagnetic or thermal radiation not taken into account in the design	
Types of entity	PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment
Risks arising from the proximity of an electromagnetic source not taken into account	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication
Medium and supports sensitive to electromagnetic or thermal radiation	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
VULNERABILITIES LINKED TO ATTACK METHOD 16 - ELECTROMAGNETIC PULSES	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance

	PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.17 INTERCEPTION OF COMPROMISING INTERFERENCE SIGNALS

Installation rules not taken into account	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV.2: Power PHY_SRV.1: Communication MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Equipment zoning not taken into account	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Equipment capable of emitting compromising stray radiation	

Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_DEP: Higher-tier organisation
No rules imposing the use of standards	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No equipment verification procedure before purchase or after maintenance work.	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No monitoring of security policy application	
Types of entity	ORG_GEN: Structure of the organisation
No information protection policy	
Types of entity	ORG_GEN: Structure of the organisation
The security policy is not applied	
Types of entity	ORG_GEN: Structure of the organisation
TEMPEST zoning not carried out	
Types of entity	PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment
Public access close to the buildings	
Types of entity	PHY_LIE.2: Premises
Room situated close to a public right-of-way	
Types of entity	PHY_LIE.3: Zone
Ancillary equipment making it easier to pick up compromising stray signals (electrical cables, pipes, etc.)	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication
No protection of access to equipment	
Types of entity	PHY_SRV.2: Power PHY_SRV.1: Communication
Medium and supports capable of emitting compromising stray radiation	
Types of entity	RES_REL: Passive or active relay

	RES_INF: Medium and supports
VULNERABILITIES LINKED TO ATTACK METHOD 17 - INTERCEPTION OF COMPROMISING STRAY SIGNALS	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.18 REMOTE SPYING

No screen saver when equipment is inactive	
Types of entity	LOG_STD: Package software or standard software

	LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Use of easily-observed passwords to access the system or application (shape on keyboard, short password)	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Password for accessing the system or application changed rarely or not at all	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Screen observable from outside	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Sensitive documents read in public places (documents observed by external persons, etc.)	
Types of entity	MAT_PAS.2: Other media
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No rules for protecting the exchange of confidential information	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
The security policy is not applied	
Types of entity	ORG_GEN: Structure of the organisation
No identification of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
The security responsibilities concerning authorisation management are not formalised.	
Types of entity	ORG_GEN: Structure of the organisation

No monitoring of application of the security policy	
Types of entity	ORG_GEN: Structure of the organisation
No information protection policy	
Types of entity	ORG_PRO: Project or system organisation
No identification of security needs for a project	
Types of entity	ORG_PRO: Project or system organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Low awareness of the need to protect information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Presence of observation point outside the site	
Types of entity	PHY_LIE.1: External environment
Zone with opening onto a public right-of-way	
Types of entity	PHY_LIE.3: Zone
Zone observable from a passage way	
Types of entity	PHY_LIE.3: Zone
VULNERABILITIES LINKED TO ATTACK METHOD 18 - REMOTE SPYING	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places

	PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.19 EAVESDROPPING

No access monitoring device when equipment is inactive	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Possibility of adding an eavesdropping programme such as a Trojan horse	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No protection of logs containing activity tracks	
Types of entity	SYS_WEB: External portal SYS_ITR: Intranet

	SYS_INT: Internet access device LOG_STD: Package software or standard software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Password for accessing the system or application changed rarely or not at all	
Types of entity	LOG_STD: Package software or standard software LOG_OS: Operating system LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No protection against the use of advanced privileges	
Types of entity	LOG_OS: Operating system
Password for accessing support software changed rarely or not at all	
Types of entity	LOG_SRV: Service, maintenance or administration software
Logical access to equipment allowing eavesdropping software to be installed	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Equipment with a communication interface that can be eavesdropped (infrared, 802.11, Bluetooth, etc.)	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No rules for protecting the exchange of confidential information	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No monitoring of application of the security policy	
Types of entity	ORG_GEN: Structure of the organisation
No identification of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
The security responsibilities concerning authorisation management are not formalised.	
Types of entity	ORG_GEN: Structure of the organisation
The security policy is not applied	
Types of entity	ORG_GEN: Structure of the organisation
No information protection policy	
Types of entity	ORG_PRO: Project or system organisation

No identification of security needs for a project	
Types of entity	ORG_PRO: Project or system organisation
Insufficient training in measures and tools for protecting external and internal exchanges	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Low awareness of the need to protect the confidentiality of information exchanges	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage through picking up information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Possibility of picking up transmissions outside the site	
Types of entity	PHY_LIE.1: External environment
No control of access to the site or premises or possibility of intrusion via indirect access routes.	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
Access to communication terminal equipment not protected	
Types of entity	PHY_SRV.1: Communication
Medium and supports whose characteristics allow eavesdropping (e.g. Ethernet, wireless communication systems)	
Types of entity	RES_INF: Medium and supports
Physical or logical access to a relay allowing eavesdropping equipment to be	

installed	
Types of entity	RES_INF: Medium and supports
No authentication of equipment connected to the network	
Types of entity	RES_INT: Communication interface
Physical access to communication support or equipment allowing eavesdropping equipment to be installed	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Communication in broadcast mode	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Complex routing between sub-networks	
Types of entity	RES_INT: Communication interface
Interface with a function that allows eavesdropping	
Types of entity	RES_INT: Communication interface
Circulating information in clear text	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
No partitioning of communication networks	
Types of entity	SYS_ITR: Intranet
Possibility of eavesdropping on exchanges with authentication servers	
Types of entity	SYS_ITR: Intranet
Possibility of eavesdropping on exchanges with application servers	
Types of entity	SYS_ITR: Intranet
Possibility of introducing eavesdropping software on client terminals	
Types of entity	SYS_MES: Electronic messaging
Possibility of installing an eavesdropping device on messaging gateways	
Types of entity	SYS_MES: Electronic messaging
Flaws in the management of access privileges to messaging gateways	
Types of entity	SYS_MES: Electronic messaging
VULNERABILITIES LINKED TO ATTACK METHOD 19 - EAVESDROPPING	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface

	RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.20 THEFT OF MEDIA OR DOCUMENTS

Single internally-developed applications	
Types of entity	LOG_APP.2: Specific business application
No equipment inventory	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Tempting equipment (trading value, technology, strategic)	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No protection of equipment against theft (anti-theft cable)	
Types of entity	MAT_ACT.1: Transportable equipment

Easily removed hard disc	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Equipment used on self-service basis by a number of persons	
Types of entity	MAT_ACT.1: Transportable equipment
Access to back-up equipment not protected	
Types of entity	MAT_ACT.3: Processing peripheral
Printer present in passage way	
Types of entity	MAT_ACT.3: Processing peripheral
Media available to everyone	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
Media sent via postal services (external service providers, internal mail service, etc.)	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
Media storage not protected	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No inventory of media used	
Types of entity	MAT_PAS.1: Electronic medium
No back-up of data contained on the media	
Types of entity	MAT_PAS.1: Electronic medium
Easily transported media (e.g. removable hard disc, back-up cartridge)	
Types of entity	MAT_PAS.1: Electronic medium
Original media	
Types of entity	MAT_PAS.2: Other media
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
Security responsibilities concerning the classification of information are not formalised or known by everyone	
Types of entity	ORG_GEN: Structure of the organisation
The security policy is not applied	
Types of entity	ORG_GEN: Structure of the organisation
No organisation for management of security incidents	
Types of entity	ORG_GEN: Structure of the organisation

No identification of sensitive assets	
Types of entity	ORG_GEN: Structure of the organisation
No monitoring of sensitive assets	
Types of entity	ORG_GEN: Structure of the organisation
No monitoring of application of the security policy	
Types of entity	ORG_GEN: Structure of the organisation
No identification of security needs for a project	
Types of entity	ORG_PRO: Project or system organisation
No information protection policy	
Types of entity	ORG_PRO: Project or system organisation
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Failure to follow rules concerning information classification.	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Low awareness of the need to protect confidential documents, leading to a lack of vigilance	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage through disclosing information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_DEC: Decision maker
No individual commitment to protect confidential documents	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Media or documents sent or present outside the site	
Types of entity	PHY_LIE.1: External environment
No control of access to the site or premises or possibility of intrusion via indirect	

access routes.	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
VULNERABILITIES LINKED TO ATTACK METHOD 20 - THEFT OF MEDIA OR DOCUMENTS	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.21 THEFT OF EQUIPMENT

No substitution equipment	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No equipment inventory	
Types of entity	MAT_ACT.3: Processing peripheral MAT_ACT.1: Transportable equipment
Equipment freely available to a number of persons	
Types of entity	MAT_ACT.1: Transportable equipment
Tempting equipment (trading value, technology, strategic)	
Types of entity	MAT_ACT.3: Processing peripheral MAT_ACT.1: Transportable equipment
Equipment that can be resold (no marking, used without password)	
Types of entity	MAT_ACT.1: Transportable equipment
Easily dismantled equipment	
Types of entity	MAT_ACT.2: Fixed equipment
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No organisation for management and treatment of security incidents linked to theft	
Types of entity	ORG_GEN: Structure of the organisation
No monitoring of application of the security policy	
Types of entity	ORG_GEN: Structure of the organisation
No rules for checking equipment entering/leaving the organisation	
Types of entity	ORG_GEN: Structure of the organisation
No identification of sensitive assets	
Types of entity	ORG_GEN: Structure of the organisation
No identification of security needs for a project	
Types of entity	ORG_PRO: Project or system organisation
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Low awareness of the need to protect equipment outside the organisation	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance

	PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Failure to follow the rules concerning physical protection of transportable equipment	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage through selling equipment	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	
Types of entity	PHY_LIE.1: External environment
No control of access to the site or premises or possibility of intrusion via indirect access routes.	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
VULNERABILITIES LINKED TO ATTACK METHOD 21 - THEFT OF EQUIPMENT	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users

	PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.22 RETRIEVAL OF RECYCLED OR DISCARDED MEDIA

Presence of residual data used by the software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Presence of residual data unknown to the user of reallocated or discarded equipment	
Types of entity	MAT_PAS.1: Electronic medium MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No means of destroying the media	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No identification of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No monitoring of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation

	ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No monitoring of application of the security policy	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No information protection policy applicable to recycling and discarding	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No contractual clauses covering the security measures to be observed by subcontractors and suppliers	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Failure to comply with rules concerning the destruction of media containing classified information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No information or awareness concerning residual data on media	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage through disclosing information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Presence of discarded media outside the site	
Types of entity	PHY_LIE.1: External environment

Presence of discarded media in public places	
Types of entity	PHY_LIE.2: Premises
Presence of discarded media in zones accessible to persons who have no need to know	
Types of entity	PHY_LIE.3: Zone
VULNERABILITIES LINKED TO ATTACK METHOD 22 - RETRIEVAL OF RECYCLED OR DISCARDED MEDIA	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.23 DISCLOSURE

No verification of approved shared access	
Types of entity	MAT_ACT.2: Fixed equipment LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Procedures for managing access privileges too heavy to operate	
Types of entity	MAT_ACT.2: Fixed equipment LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Access right management functions too complicated to use and capable of producing an error	
Types of entity	MAT_ACT.2: Fixed equipment
Presence of shared directory for storing information	
Types of entity	MAT_ACT.2: Fixed equipment
Media can be used to exchange sensitive information	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No structure responsible for defining, implementing and monitoring access privileges to information	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No identification of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
The security policy is not applied	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No personal commitment to protect confidentiality	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation

Procedures for managing and applying authorisation too heavy to use	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation

Security responsibilities concerning the classification of information are not formalised or known by everyone	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation

No monitoring of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation

No information protection policy	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation

Failure to observe information classification rules	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel

No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel

Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel

Inadequate awareness of the need to protect sensitive information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel

Failure to observe discretion	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker

	PER: Personnel
Obtaining an advantage through disclosing information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No checking (or tracking) of exchanges with the outside	
Types of entity	PHY_SRV.1: Communication PHY_LIE.3: Zone PHY_LIE.2: Premises
Presence of a communication network with the outside allowing exchange of information	
Types of entity	RES_INF: Medium and supports
Complex or unpractical files	
Types of entity	RES_INT: Communication interface
Standard interface allowing information exchanges (e.g. Bluetooth interface accepting all communications by default)	
Types of entity	RES_INT: Communication interface
Resources can be used without tracking	
Types of entity	RES_INT: Communication interface
No user notification	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Complex routing between sub-networks	
Types of entity	RES_INT: Communication interface
No strict routing between sub-networks	
Types of entity	RES_INT: Communication interface
No filtering and logging on communication relays between networks	
Types of entity	RES_REL: Passive or active relay
The system is connected to external networks	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
No control of access to information stored in the directory	
Types of entity	SYS_ANU: Company directory
No access logging	
Types of entity	SYS_INT: Internet access device
No filtering system	
Types of entity	SYS_INT: Internet access device

Access privileges to shared information difficult to manage or not managed at all (definition, implementation, monitoring)	
Types of entity	SYS_ITR: Intranet
No partitioning of communication networks	
Types of entity	SYS_ITR: Intranet
No measure to avoid negligence when information is sent	
Types of entity	SYS_MES: Electronic messaging
The system can be used by all personnel	
Types of entity	SYS_MES: Electronic messaging
The system allows attachments to be exchanged	
Types of entity	SYS_MES: Electronic messaging
No effective and operational virus shield	
Types of entity	SYS_MES: Electronic messaging
No management of information access privileges (possibility of corrupting public data, etc.)	
Types of entity	SYS_WEB: External portal
The system makes it easy to disclose information to the outside	
Types of entity	SYS_WEB: External portal
VULNERABILITIES LINKED TO ATTACK METHOD 23 - DISCLOSURE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation

	ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.24 DATA FROM UNTRUSTWORTHY SOURCES

Software retrieval from a non-authenticated source	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

Possibility of installing correction programmes, updates, patches, hotfixes, etc.	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

No sure means of identification	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application

No storage of activity tracks	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application

No means of guaranteeing the source of equipment	
Types of entity	MAT_ACT: Data processing equipment (active)

	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_DEP: Higher-tier organisation
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No means of guaranteeing the source of supplies	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No monitoring of application of the security policy	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No policy for storing and analysing activity tracks	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No information concerning the division of responsibility and means of guaranteeing the legitimacy of a request.	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No structure allowing identification of a person to be guaranteed within the organisation or a project	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No awareness programme concerning the risks of usurping of identity (misuse of means of authentication such as passwords)	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Credulity	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Failure to appreciate the importance of qualifying information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users

	PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Conflictual industrial relations	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Obtaining an advantage through misinforming	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
No means of guaranteeing the authenticity of codes	
Types of entity	PER_DEV: Developer
Unfamiliarity with security measures	
Types of entity	PER_DEV: Developer
Possibility of corrupting a communication	
Types of entity	RES_INF: Medium and supports
Protocol not allowing safe authentication of the sender of a communication	
Types of entity	RES_INT: Communication interface
Resources can be used without tracking	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Assignment files too complex or unpractical	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)	
Types of entity	RES_REL: Passive or active relay
Possibility of usurping the directory function	
Types of entity	SYS_ANU: Company directory
The system does not allow the author of a modification to be identified	
Types of entity	SYS_ANU: Company directory
The system allows access to data that cannot be authenticated (e.g. hoax)	
Types of entity	SYS_INT: Internet access device
The system does has no means of preserving the activity history	
Types of entity	SYS_WEB: External portal SYS_ITR: Intranet SYS_INT: Internet access device
The system allows information to be stored or modified without authentication of the authors	
Types of entity	SYS_ITR: Intranet
The system allows information to be sent and received without authentication of the senders or recipients	

Types of entity	SYS_MES: Electronic messaging
The system has no filter to prevent hoaxes being received from the outside	
Types of entity	SYS_MES: Electronic messaging
The system allows relaying	
Types of entity	SYS_MES: Electronic messaging
The system does not allow the person issuing a request to be identified	
Types of entity	SYS_WEB: External portal
VULNERABILITIES LINKED TO ATTACK METHOD 24 - INFORMATION FROM UNTRUSTWORTHY SOURCES	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application

	LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.25 TAMPERING WITH HARDWARE

Additional hardware items can be fitted for storing, transmitting or corrupting information (e.g. physical keylogger).	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No procedure for checking work carried out by external personnel on the organisation's equipment	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No monitoring of application of the security policy	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_GEN: Structure of the organisation
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_GEN: Structure of the organisation
No operational qualification procedures	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No monitoring of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No identification of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No procedures for validating hardware components when they are delivered or returned from maintenance	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Software not adequately tested before acceptance, especially concerning limit values	
Types of entity	ORG_PRO: Project or system organisation
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer

	PER_DEC: Decision maker PER: Personnel
No vigilance when a maintenance agent works on a workstation or server	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Low awareness of the need to protect equipment outside the organisation	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage through misinforming	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	
Types of entity	PHY_LIE.1: External environment
No control of access to the site or premises or possibility of intrusion via indirect access routes.	
Types of entity	PHY_SRV.1: Communication PHY_LIE.3: Zone PHY_LIE.2: Premises
Possibility of circuit derivation	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
VULNERABILITIES LINKED TO ATTACK METHOD 25 - TAMPERING WITH HARDWARE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution

	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.26 TAMPERING WITH SOFTWARE

The remote maintenance link is permanently activated	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

Possible existence of hidden functions introduced during the design and development phase	
Types of entity	SYS_WEB: External portal SYS_ANU: Company directory LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software

	LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Possibility of modifying or corrupting the software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No protection against the use of advanced privileges	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Use of non-evaluated software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No implementation of basic security rules applicable to the operating system and software	
Types of entity	SYS_MES: Electronic messaging LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Possibility of creating or modifying system commands	
Types of entity	SYS_WEB: External portal LOG_OS: Operating system
Software retrieval from a non-authenticated source	
Types of entity	LOG_OS: Operating system
Possibility of remote administration of the system using non-encrypted administration tools	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
Connection passwords not sufficiently complex	
Types of entity	SYS_MES: Electronic messaging LOG_OS: Operating system

Possibility of installing correction programmes, updates, patches, hotfixes, etc.	
Types of entity	LOG_OS: Operating system
Possibility of remote system administration	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
Use of a standard operating system on which logical attacks have already been carried out	
Types of entity	LOG_OS: Operating system
Possibility of remote system administration from any station	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
Possibility of deleting, modifying or installing new programmes	
Types of entity	LOG_OS: Operating system
The SNMP layer is activated	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
The equipment can be booted from any peripheral (e.g. floppy disc, CD-ROM)	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No means of checking the safety of media when they enter the organisation	
Types of entity	MAT_PAS.1: Electronic medium
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_DEP: Higher-tier organisation
No procedure for checking work carried out by external personnel on the organisation's equipment	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No contractual clauses guaranteeing the safety of supplies delivered by a subcontractor or supplier	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No global policy for fighting against malicious code	
Types of entity	ORG_GEN: Structure of the organisation
No identification of sensitive assets	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No monitoring of application of the security policy	

Types of entity	ORG_GEN: Structure of the organisation
No monitoring of sensitive assets	
Types of entity	ORG_GEN: Structure of the organisation
No policy for protecting the workstations	
Types of entity	ORG_GEN: Structure of the organisation
No policy for storing and analysing activity tracks	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No measures for checking developments	
Types of entity	ORG_PRO: Project or system organisation
No measures for protecting code integrity during the design, installation and operation phases	
Types of entity	ORG_PRO: Project or system organisation
Use of software without a guarantee of its source	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Conflictual industrial relations	
Types of entity	PER_UTI: Users PER_DEC: Decision maker
Low awareness of the threat posed by malicious codes	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Correct reflex actions not known if an anomaly is detected	
Types of entity	PER_UTI: Users PER_DEC: Decision maker
Failure to comply with anti-virus software updating rules	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Obtaining an advantage through disrupting the information system	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Conflictual situation	
Types of entity	PER_EXP: Operator / Maintenance

	PER_DEV: Developer
Unfamiliarity with security measures	
Types of entity	PER_DEV: Developer
No means of guaranteeing the authenticity of developments	
Types of entity	PER_DEV: Developer
Operator or maintainer with extended privileges	
Types of entity	PER_EXP: Operator / Maintenance
Unfamiliarity with emergency procedures if an anomaly is detected	
Types of entity	PER_EXP: Operator / Maintenance
Use of equipment outside the organisation (personnel's homes, another organisation, etc.)	
Types of entity	PHY_LIE.1: External environment
No control of access to the site or premises or possibility of intrusion via indirect access routes.	
Types of entity	PHY_SRV.1: Communication PHY_LIE.3: Zone PHY_LIE.2: Premises
The network makes it easy for unauthorised persons to use the resources	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Assignment files too complex or unpractical	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Possibility of adding software derivations	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The network allows the system resources to be modified or adjusted	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Additional software can be added for storing, transmitting or corrupting information (e.g. keylogger)	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Resources can be used without tracking	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Applications can be modified or changed	
Types of entity	SYS_WEB: External portal SYS_ANU: Company directory
Programmes or system files can be deleted or modified	
Types of entity	SYS_WEB: External portal SYS_ANU: Company directory
No awareness programme concerning risks incurred through downloading software	

Types of entity	SYS_INT: Internet access device
No anti-virus check on exchanges	
Types of entity	SYS_INT: Internet access device
The system allows asynchronous operation of certain parts or commands of the operating system (e.g. JavaScript components exploring the hard disc content)	
Types of entity	SYS_INT: Internet access device
Presence of a device allowing remote modification or installation of applications	
Types of entity	SYS_ITR: Intranet
Use of shared storage space	
Types of entity	SYS_ITR: Intranet
Use of an obsolete version of the messaging server	
Types of entity	SYS_MES: Electronic messaging
Use of a distribution list that includes a large part of the personnel	
Types of entity	SYS_MES: Electronic messaging
Presence of protocol that has no authentication function	
Types of entity	SYS_MES: Electronic messaging
The messaging system allows automatic message transmission	
Types of entity	SYS_MES: Electronic messaging
No awareness programme concerning the risks incurred by opening attachments	
Types of entity	SYS_MES: Electronic messaging
The system allows asynchronous operation of certain parts or commands of the operating system to be exploited (e.g. automatic opening of attachments)	
Types of entity	SYS_MES: Electronic messaging
Applications are not checked before installation	
Types of entity	SYS_MES: Electronic messaging
The messaging system allows software updates to be installed (e.g. patches, anti-virus updates, etc.)	
Types of entity	SYS_MES: Electronic messaging
No anti-virus filtering system	
Types of entity	SYS_MES: Electronic messaging
Pirated programmes can be installed	
Types of entity	SYS_WEB: External portal
VULNERABILITIES LINKED TO ATTACK METHOD 26 - TAMPERING WITH SOFTWARE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface

	RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.27 POSITION DETECTION

Locatable equipment (e.g. triangulation)	
Types of entity	MAT_ACT.1: Transportable equipment
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No rules for protecting the confidentiality of information that can be used to locate a personnel member (ticket requests, entry/exit records, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance

	PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Lack of discretion or vigilance	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
VULNERABILITIES LINKED TO ATTACK METHOD 27 - POSITION DETECTION	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment

	MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.28 EQUIPMENT FAILURE

No diagnostic function to prevent equipment failures	
Types of entity	LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system
No protection against electrical disturbances	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Incorrect operating conditions	
Types of entity	RES_INF: Medium and supports MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Maintenance fault	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Poor equipment reliability	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Ageing of the equipment	

Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Medium unsuitable for the life of data to be stored	
Types of entity	MAT_PAS.1: Electronic medium
Poor storage conditions	
Types of entity	MAT_PAS.1: Electronic medium
No clause covering response time for repair and replacement in the event of equipment failure	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
Maintenance contract monitoring not organised	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No monitoring of maintenance and support contracts with suppliers	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No failure reporting (volumes, cost of incidents, downtime)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No rules covering conditions of use of information processing infrastructures (ban on smoking, drinks and food in rooms housing IT equipment)	
Types of entity	ORG_GEN: Structure of the organisation
No continuity plan covering the organisation's essential activities	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No quick response instructions to protect equipment in the event of water damage or fire	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Analysis of match between needs and equipment capabilities not organised	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No rules covering conditions of use of information processing infrastructures (ban on smoking, drinks and food in rooms housing IT equipment)	
Types of entity	ORG_PRO: Project or system organisation
No implementation of incident monitoring to foresee failures or saturation (trend charts)	
Types of entity	PER_EXP: Operator / Maintenance PER_DEC: Decision maker
No passing up of information for a centralised failure analysis	
Types of entity	PER_UTI: Users

Unfamiliarity with the instructions for using the equipment	
Types of entity	PER_UTI: Users
Failure to take into account a specific environment that increases the risks of failure (overheated atmosphere, industrial environment, etc.)	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No checking to confirm that emergency resources operate correctly	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication
Manual triggering of the emergency solution	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication
Poor medium reliability	
Types of entity	RES_INF: Medium and supports
Ageing of the medium	
Types of entity	RES_INF: Medium and supports
VULNERABILITIES LINKED TO ATTACK METHOD 28 - EQUIPMENT FAILURE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation

	ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.29 EQUIPMENT MALFUNCTION

No diagnostic function to prevent equipment failures	
Types of entity	LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system
No protection against electrical disturbances	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Incorrect operating conditions	
Types of entity	RES_INF: Medium and supports MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Poor equipment reliability	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Possibility of incompatibility between equipment items	
Types of entity	MAT_ACT: Data processing equipment (active)

	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Medium unsuitable for the life of data to be stored	
Types of entity	MAT_PAS.1: Electronic medium
Poor storage conditions	
Types of entity	MAT_PAS.1: Electronic medium
No incident monitoring to foresee failures or saturation (trend charts)	
Types of entity	ORG_DEP: Higher-tier organisation
No rules imposing the use of standards	
Types of entity	ORG_DEP: Higher-tier organisation
No clause covering response time for repair and treatment in the event of malfunction	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No reporting on malfunctions	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No continuity plan covering the organisation's essential activities	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No operational qualification procedures	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No rules covering the operating environment of information processing infrastructures (temperature, humidity, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Analysis of match between needs and equipment capabilities not organised	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No implementation of incident monitoring to foresee failures or saturation (trend charts)	
Types of entity	PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Unfamiliarity with the instructions for using the equipment	
Types of entity	PER_UTI: Users
No passing up of information for a centralised failure analysis	
Types of entity	PER_UTI: Users
Failure to take into account a specific environment that increases the risks of failure (overheated atmosphere, industrial environment, etc.)	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No checking to confirm that emergency resources operate correctly	
Types of entity	PHY_SRV: Essential service

	PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication
Manual triggering of the emergency solution	
Types of entity	PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication
Ageing of the medium	
Types of entity	RES_INF: Medium and supports
Possibility of incompatibility between the media and other components	
Types of entity	RES_INF: Medium and supports
Medium and supports with technical characteristics specific to their locality (e.g. different ADSL configuration parameters between France and the United Kingdom)	
Types of entity	RES_INF: Medium and supports
Poor medium reliability	
Types of entity	RES_INF: Medium and supports
Maintenance fault	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
Interface with technical characteristics specific to the country (e.g. different telephone connectors between France and the United Kingdom)	
Types of entity	RES_INT: Communication interface
Possibility of incorrect configuration, installation or modification of relays	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Ageing of the equipment	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Possibility of incompatibility between resources	
Types of entity	RES_INT: Communication interface
VULNERABILITIES LINKED TO ATTACK METHOD 29 - EQUIPMENT MALFUNCTION	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution

	PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.30 SATURATION OF THE INFORMATION SYSTEM

No filter to protect the system against saturation	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Unnecessary use of resources	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Application requiring computing resources not matched by the equipment (e.g.	

insufficient RAM)	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Requirements defined for a project without taking into account special situations that put the system under limit conditions.	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No qualification of developments in a context representative of operation	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Incorrect sizing of resources (e.g. insufficient reserve time on a laptop battery).	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Unwanted persistence of data on media	
Types of entity	MAT_PAS.1: Electronic medium
No rules imposing the use of standards	
Types of entity	ORG_DEP: Higher-tier organisation
No incident monitoring to foresee failures or saturation (trend charts)	
Types of entity	ORG_DEP: Higher-tier organisation
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)	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No policy for checking the correct sizing of the equipment of the information processing infrastructure, including the emergency equipment	

Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No instructions for avoiding the use of IT resources in a manner that leads to saturation of storage spaces or processing resources.	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No instructions relating to incidents (detection, action, etc.)	
Types of entity	ORG_GEN: Structure of the organisation
No decision to resize when significant increases in the use of IT resources are observed.	
Types of entity	PER_DEC: Decision maker
No implementation of incident monitoring to foresee failures or saturation (trend charts)	
Types of entity	PER_EXP: Operator / Maintenance
Insufficient training in the correct use of the information tool (disturbance of the system, installation of incompatible software, etc.)	
Types of entity	PER_UTI: Users
Obtaining an advantage through disrupting the information system	
Types of entity	PER_UTI: Users
Low awareness of the need to economise the organisation's IT resources (poor use of storage spaces, etc.)	
Types of entity	PER_UTI: Users
Incorrect sizing of telecommunication resources, resulting, for example, from daily use of resources intended for the emergency solution.	
Types of entity	PHY_SRV.1: Communication
Incorrect sizing of emergency resources	
Types of entity	PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power
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.)	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Possibility of incorrect configuration, installation or modification of relays	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Incorrect sizing (e.g. too much data for the maximum passband)	
Types of entity	RES_REL: Passive or active relay
Incorrect sizing of resources (e.g. too many users for the maximum capacity of the directory)	
Types of entity	SYS_ANU: Company directory
Possibility of subjecting the system to an unlimited number of requests	
Types of entity	SYS_WEB: External portal SYS_ITR: Intranet

	SYS_INT: Internet access device SYS_ANU: Company directory
Existence of periods or events that cause a very significant increase in use of the system	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ANU: Company directory
Incorrect sizing of resources (e.g. too many users for the number of connections possible and the passband)	
Types of entity	SYS_INT: Internet access device
No management of write rights in shared storage spaces.	
Types of entity	SYS_ITR: Intranet
Incorrect sizing of resources (e.g. not enough storage or file share space)	
Types of entity	SYS_ITR: Intranet
No partitioning of communication networks	
Types of entity	SYS_ITR: Intranet
Use of the internal distribution list accessible to everyone	
Types of entity	SYS_MES: Electronic messaging
Incorrect sizing of storage spaces for received messages	
Types of entity	SYS_MES: Electronic messaging
The messaging system allows automatic message transmission	
Types of entity	SYS_MES: Electronic messaging
No protection against spam	
Types of entity	SYS_MES: Electronic messaging
No limits on the size of attachments	
Types of entity	SYS_MES: Electronic messaging
Incorrect use of the messaging service (mailboxes used as storage space)	
Types of entity	SYS_MES: Electronic messaging
Public access to the gateway	
Types of entity	SYS_WEB: External portal
Incorrect sizing of resources (e.g. too many simultaneous connections)	
Types of entity	SYS_WEB: External portal
VULNERABILITIES LINKED TO ATTACK METHOD 30 - SATURATION OF THE INFORMATION SYSTEM	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports

	RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.31 SOFTWARE MALFUNCTION

Possible side effects after updating a software component	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No storage of processing tracks	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application

	LOG_APP.1: Standard business application LOG: Software
Lack of training in maintaining and operating new equipment	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No maintenance procedure	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No systematic qualification procedure before installation or updating	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No clock synchronisation procedure	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No passing up of information for a centralised malfunction analysis	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Possibility of incorrect configuration, installation or modification of the operating system	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software

	LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No report for maintenance operations	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Configuration of software components not managed or prone to management errors (e.g. application of a UK patch not adapted to a FR version)	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Documentation not up to date	
Types of entity	LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Applications are not checked before installation	
Types of entity	SYS_MES: Electronic messaging LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system
Use of an obsolete version of the operating system or applications	
Types of entity	SYS_MES: Electronic messaging LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system
No rules imposing the use of standards	
Types of entity	ORG_DEP: Higher-tier organisation
No incident monitoring to foresee failures or saturation (trend charts)	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses covering support and call-out conditions	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No policy for partitioning user environments to avoid unintentional assignment of rights to modify the system and application	
Types of entity	ORG_GEN: Structure of the organisation
No instructions aimed at eliminating risk-inducing behaviour in the use of information	

resources	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No instructions relating to incidents (detection, action, etc.)	
Types of entity	ORG_GEN: Structure of the organisation
No continuity plan covering the organisation's essential activities	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
The computing equipment is not homogenous	
Types of entity	ORG_GEN: Structure of the organisation
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)	
Types of entity	ORG_PRO: Project or system organisation
No incident monitoring to foresee malfunctions (trend charts)	
Types of entity	PER_DEC: Decision maker
Lack of training	
Types of entity	PER_DEV: Developer
No security rules for developments	
Types of entity	PER_DEV: Developer
No training in the use and maintenance of new software	
Types of entity	PER_EXP: Operator / Maintenance
Incorrect sizing of operating and maintenance resources	
Types of entity	PER_EXP: Operator / Maintenance
Failure to follow work procedures	
Types of entity	PER_EXP: Operator / Maintenance
Insufficient training in the correct use of the information tool (disturbance of the system, installation of incompatible software, etc.)	
Types of entity	PER_UTI: Users
Possibility of incorrect configuration, installation or modification of relays	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Poor management of pilot releases and configurations	
Types of entity	RES_INT: Communication interface
Interface side effects (compatibility problems between protocols, etc.)	
Types of entity	RES_INT: Communication interface
Possibility of the system being subjected to badly formed requests and data (e.g. buffer overflow, denial of service on LDAP server)	
Types of entity	SYS_ITR: Intranet SYS_ANU: Company directory
Failure to comply with installation or maintenance procedures.	

Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory
Possibility of subjecting the system to an unlimited number of requests	
Types of entity	SYS_INT: Internet access device
Software incompatibility (e.g. side effect of message-filtering anti-virus software, etc.)	
Types of entity	SYS_MES: Electronic messaging
Possibility of the system being subjected to badly formed requests and data (e.g. buffer overflow, denial of service on SMTP, POP3, IMAP server)	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging
Use of an obsolete version of the messaging server	
Types of entity	SYS_MES: Electronic messaging
VULNERABILITIES LINKED TO ATTACK METHOD 31 - SOFTWARE MALFUNCTION	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active)

	MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.32 BREACH OF INFORMATION SYSTEM MAINTAINABILITY

Applications are not checked before installation	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No emergency procedure	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No backtrack procedure in the event of a modification error	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No maintenance procedure	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Documentation not up to date	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software

	LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No report of maintenance operations	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No storage of processing and modification tracks	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Specific software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No training in the use and maintenance of new software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Obsolete software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Non-upgradable software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software

	LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Inaccessibility of support media outside the organisation or from a country with a large time difference	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Non-upgradable hardware	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Obsolete hardware	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Specific hardware	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Back-up hardware, software or procedures modified without taking old back-ups or archives into account	
Types of entity	MAT_PAS.1: Electronic medium
Obsolete medium	
Types of entity	MAT_PAS.1: Electronic medium
Loss or poor management of original documents (support contracts, licences, etc.)	
Types of entity	MAT_PAS.2: Other media
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clause covering the activity (in the event of shutting down the activity, supplier bankruptcy, etc.)	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No guarantee of the organisation's durability	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No monitoring of maintenance and support contracts with suppliers	
Types of entity	ORG_PRO: Project or system organisation

	ORG_GEN: Structure of the organisation
No instructions relating to incidents (detection, action, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No Quality Assurance Manual	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No organisation for protecting documentation and system maintenance resources	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No continuity plan covering the organisation's essential activities	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No procedures for system configuration management	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No use of norms or standards relating to information system development	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No training plan for maintenance of new systems	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Technology chosen without guarantee of continuity	
Types of entity	PER_DEC: Decision maker
Low maintenance budget	
Types of entity	PER_DEC: Decision maker
Existence of obsolete components in the information processing infrastructure (development in languages no longer used, etc.)	
Types of entity	PER_DEC: Decision maker
Failure to comply with quality rules	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
No standard or norm	
Types of entity	PER_DEV: Developer
Failure to comply with development rules	
Types of entity	PER_DEV: Developer
Insufficient training in the correct use of the information tool (disturbance of the system, installation of incompatible software, etc.)	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance
Use of software or developments outside the organisation's norms and standards	

Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance
Maintenance fault	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
No cable layout plan	
Types of entity	RES_INF: Medium and supports
Maintenance or use of the equipment only possible if network supports are available	
Types of entity	RES_INF: Medium and supports
System maintained or operated via the network	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
No maximum response time for support guarantees	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Use of an obsolete version of the operating system or applications	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
Use of an obsolete version of the messaging server	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
Use of an obsolete system	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
Use of a non-standard system	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
No monitoring of installation and maintenance procedures (configuration and parameter setting records)	

Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
No internal support tool	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
VULNERABILITIES LINKED TO ATTACK METHOD 32 - BREACH OF INFORMATION SYSTEM MAINTAINABILITY	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware

	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.33 UNAUTHORISED USE OF EQUIPMENT

No management of licences or registration and activation measures	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Possibility of installing a backdoor or Trojan horse in the operating system	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Shared use of connection identifier	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Resource sharing makes it easy for unauthorised persons to use the system	
Types of entity	LOG_OS: Operating system
The system is connected to external networks	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
The equipment can be used for purposes other than those intended (development of software for use outside the organisation, etc.)	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Media available to everyone	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium

Responsibilities for information systems security not dealt with in the internal regulations	
Types of entity	ORG_DEP: Higher-tier organisation
No security policy for protecting the information processing infrastructure in the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_DEP: Higher-tier organisation
No awareness of the risks of sanction	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
No contractual clauses relating to the use of IT equipment	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions concerning the use of IT equipment	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Possibility of using the organisation's resources without supervision (self-service equipment, etc.)	
Types of entity	ORG_GEN: Structure of the organisation
No monitoring procedure	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
The security policy is not applied	
Types of entity	ORG_GEN: Structure of the organisation
No IT charter specifying the rules of use	
Types of entity	PER_EXP: Operator / Maintenance PER_DEV: Developer ORG_GEN: Structure of the organisation
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Personnel not aware of the risks of sanction	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Rights assigned without legitimate need	
Types of entity	PER_UTI: Users PER_DEC: Decision maker

Obtaining an advantage	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Failure to comply with the IT charter specifying the rules of use	
Types of entity	PER_UTI: Users PER_DEV: Developer PER_DEC: Decision maker
Insufficient monitoring of material requirements for developing an application	
Types of entity	PER_DEV: Developer
No code of conduct	
Types of entity	PER_DEV: Developer
No management of the equipment assets	
Types of entity	PER_EXP: Operator / Maintenance
No procedures for checking authorisation of personnel entering the site or premises	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No procedures for checking the identity of all persons entering the premises or zones	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No logging of entry to the site	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No measures to make communication lines and equipment secure	
Types of entity	PHY_SRV.1: Communication
The equipment allows system resources to be used from outside	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
The equipment can be accessed by everyone	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
The equipment is connected to external networks	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
The system can be used for purposes other than those intended	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface

	RES_INF: Medium and supports RES: Network
The equipment can be used for purposes other than those intended	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
No audit or supervision of accesses (for example inventory of accesses outside the organisation and types of data flow)	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
No access rules	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The system is connected to external networks	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The system can be accessed by everyone	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
VULNERABILITIES LINKED TO ATTACK METHOD 33 - UNAUTHORISED USE OF EQUIPMENT	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface

	RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.34 FRAUDULENT COPYING OF SOFTWARE

No management of profile privileges (administrators, users, guest, etc.)	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No management of licences or registration and activation measures	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software

	LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
Tempting or popular software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Software can be easily copied	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Proprietary operating system distributions can be easily copied	
Types of entity	LOG_OS: Operating system
Tempting or popular operating system	
Types of entity	LOG_OS: Operating system
Equipment allowing data to be recorded on media (floppy disc, ZIP disc, CD/DVD writer)	
Types of entity	MAT_ACT.1: Transportable equipment
Equipment allowing data to be recorded on media (floppy disc, ZIP disc, CD/DVD writer)	
Types of entity	MAT_ACT.2: Fixed equipment
Lack of information concerning laws and regulations applicable to information processing	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation
Responsibilities for information systems security not dealt with in the internal regulations	
Types of entity	ORG_DEP: Higher-tier organisation
No licence monitoring policy imposed at the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses concerning the use of fraudulent copies of software	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No IT charter specifying the rules of use	
Types of entity	ORG_GEN: Structure of the organisation
No awareness of the risks of sanction	

Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No awareness or information concerning copyright law	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No monitoring procedure	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
The security policy is not applied	
Types of entity	ORG_GEN: Structure of the organisation
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Failure to comply with the IT charter specifying the rules of use	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
Personnel not aware of the risk of sanction	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEC: Decision maker
No procedures for checking the identity of all persons entering the premises or zones	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No procedures for checking authorisation of personnel entering the site or the premises	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No logging of entry to the site	
Types of entity	PHY_LIE.3: Zone

	PHY_LIE.2: Premises
The origin of applications is not checked before installation	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The access system allows software storage	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The access system allows software downloads	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
VULNERABILITIES LINKED TO ATTACK METHOD 34 - FRAUDULENT COPYING OF SOFTWARE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation

	ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.35 USE OF COUNTERFEIT OR COPIED SOFTWARE

No management of licences or registration and activation measures	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Software can be easily copied	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Tempting or popular software	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Possibility of the systems operating with illegally copied or counterfeit operating systems	
Types of entity	LOG_OS: Operating system
Responsibilities for information systems security not dealt with in the internal regulations	
Types of entity	ORG_DEP: Higher-tier organisation
No licence monitoring policy imposed at the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
Contract contains no clauses concerning identification and verification of the origin of	

the software.	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No awareness or information concerning copyright law	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No monitoring of product certification	
Types of entity	ORG_GEN: Structure of the organisation
No monitoring of product origin	
Types of entity	ORG_GEN: Structure of the organisation
No IT charter specifying the rules of use	
Types of entity	ORG_GEN: Structure of the organisation
The security policy does not include reminding all personnel of their obligations and responsibilities in civil, criminal and regulatory matters.	
Types of entity	ORG_GEN: Structure of the organisation
No definition of privileges limiting the possibility of installing software on workstations	
Types of entity	ORG_PRO: Project or system organisation
Personnel not aware of the risk of sanction	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Failure to comply with the IT charter specifying the rules of use	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No product certification	
Types of entity	PER_DEV: Developer
No procedure for assessing products	
Types of entity	PER_DEV: Developer

No procedure and means of verifying the origin of the software (code signature, binary signature, etc.)	
Types of entity	PER_DEV: Developer
No logging of entry to the site	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No procedures for checking authorisation of personnel entering the site or the premises	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No procedures for checking the identity of all persons entering the premises or zones	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
The origin of applications is not checked before installation	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The access system allows software storage	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The access system allows software downloads	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
VULNERABILITIES LINKED TO ATTACK METHOD 35 - USE OF COUNTERFEIT OR COPIED SOFTWARE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service

	PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.36 CORRUPTION OF DATA

No monitoring of data integrity	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

No procedure or system for authorising personnel to modify data	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

The remote maintenance link is permanently activated

Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application

No restriction on software entry points

Types of entity	LOG_STD: Package software or standard software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application

Applications are not checked before installation

Types of entity	SYS_MES: Electronic messaging LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application

No implementation of basic security rules applicable to the operating system and software

Types of entity	SYS_MES: Electronic messaging LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application

The operating system allows access to data (data base, etc.)

Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application

Possibility of remote system administration from any station

Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system

Possibility of remote administration of the system using non-encrypted administration tools

Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface

	LOG_OS: Operating system
The software allows access to data (content of hard disc, data base, etc.)	
Types of entity	LOG_OS: Operating system
Connection passwords not sufficiently complex	
Types of entity	SYS_MES: Electronic messaging LOG_OS: Operating system
The operating system is not checked before installation	
Types of entity	LOG_OS: Operating system
Resource sharing makes it easy for unauthorised persons to use the system	
Types of entity	LOG_OS: Operating system
Possibility of remote system administration	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
The SNMP layer is activated	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
No data protection rules	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
The equipment can be booted from any peripheral (e.g. floppy disc, CD-ROM)	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Obsolete hardware	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No back-up redundancy or procedure	
Types of entity	MAT_ACT.2: Fixed equipment
Wear of media	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT.3: Processing peripheral
No means of protecting and monitoring data integrity	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT.3: Processing peripheral
No rules and procedures for personnel authorisation	
Types of entity	ORG_GEN: Structure of the organisation

	ORG_DEP: Higher-tier organisation
No authorisation management and monitoring policy imposed at the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No information protection policy imposed at the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
Responsibilities for information systems security not dealt with in the internal regulations	
Types of entity	ORG_DEP: Higher-tier organisation
No policy for authorising access to information	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
Accesses to the IS are not secured (gateways, intrusion detection, supervision of security events, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
No contractual clauses relating to the protection of IT equipment	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No monitoring of application of the security policy	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No instructions concerning the use of IT equipment	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No prevention and detection of viruses and other malicious programmes	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No access control to information	
Types of entity	ORG_GEN: Structure of the organisation
No training plan concerning security issues	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No procedures for checking external floppy disks	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No IT charter specifying the rules of use	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Failure to comply with the IT charter specifying the rules of use	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance

	PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No protection and classification of information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Personnel not aware of the risk of sanction	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Personnel susceptible to enticement	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Conflictual situation between persons	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No procedures for checking the identity of all persons entering the premises or zones	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No procedures for checking authorisation of personnel entering the site or the premises	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises

No logging of entry to the site	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No measures to make communication lines and equipment secure	
Types of entity	PHY_SRV.1: Communication
No physical and logical protection (partitioning, etc.)	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
Possibility of interfering with data transmitted via the communication media	
Types of entity	RES_INF: Medium and supports
The network allows the system resources to be modified or adjusted	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The network makes it easy for unauthorised persons to use the resources	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
No robust access control system	
Types of entity	RES_REL: Passive or active relay
No back-up procedure	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_ANU: Company directory
The system allows remote deleting, modifying or installing of programmes	
Types of entity	SYS_ITR: Intranet SYS_INT: Internet access device
The system allows hostile software such as Trojan horses, viruses, worms, logic bombs, etc. to be introduced	
Types of entity	SYS_ITR: Intranet SYS_INT: Internet access device
The system allows asynchronous operation of certain parts or commands of the operating system (e.g. JavaScript components exploring the hard disc content)	
Types of entity	SYS_ITR: Intranet SYS_INT: Internet access device
No partitioning of communication networks	
Types of entity	SYS_ITR: Intranet
The system allows asynchronous operation of certain parts or commands of the operating system to be exploited (e.g. automatic opening of attachments)	
Types of entity	SYS_MES: Electronic messaging
No audit or supervision of accesses	
Types of entity	SYS_WEB: External portal

No access rules	
Types of entity	SYS_WEB: External portal
VULNERABILITIES LINKED TO ATTACK METHOD 36 - DATA CORRUPTION	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.37 ILLEGAL PROCESSING OF DATA

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

Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No encryption system	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Possibility of installing a backdoor or Trojan horse in the operating system	
Types of entity	LOG_STD: Package software or standard software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	
Types of entity	LOG_OS: Operating system
Possibility of installing a backdoor or Trojan horse in the operating system	
Types of entity	LOG_SRV: Service, maintenance or administration software
No physical protection	
Types of entity	MAT_ACT.3: Processing peripheral
No means of identifying the sensitivity of information contained on the media	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
Media available to everyone	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
Tempting equipment (trading value, technology, strategic)	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
Easily transported or removable media (e.g. floppy disc, ZIP disc, removable hard disc)	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No means of encryption	
Types of entity	MAT_PAS.1: Electronic medium
No procedure and means for destruction	

Types of entity	MAT_PAS.1: Electronic medium
Lack of information concerning laws and regulations applicable to information processing	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_DEP: Higher-tier organisation
No subject in the internal regulations dealing with responsibilities for information systems security	
Types of entity	ORG_DEP: Higher-tier organisation
No information protection policy imposed at the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
No confidentiality clause in the contract	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No provisions for monitoring and sanctioning	
Types of entity	ORG_PRO: Project or system organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
No instructions relating to incidents (detection, action, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No access control to information	
Types of entity	ORG_GEN: Structure of the organisation
Lack of awareness of individual responsibilities	
Types of entity	ORG_GEN: Structure of the organisation
No one responsible for the protection of personal data and information	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
The security policy is not applied especially in relation to processing of personal information	
Types of entity	ORG_GEN: Structure of the organisation
Lack of personnel awareness	
Types of entity	ORG_PRO: Project or system organisation
No protection and audit of access to sensitive information	
Types of entity	ORG_PRO: Project or system organisation
Personnel not aware of the risk of sanction	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No training to explain the conditions controlling the lawful use of information	

Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No protection and classification of information	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Unfamiliarity with security measures	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Access point allowing unlawful eavesdropping	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
No identification of the system protection levels	
Types of entity	SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory
No content monitoring	
Types of entity	SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory
No audit or supervision of accesses	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory
No management of access authorisation	
Types of entity	SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory
The system makes it easy to disclose information to the outside	
Types of entity	SYS_MES: Electronic messaging SYS_INT: Internet access device SYS_ANU: Company directory
The system is connected to external networks	

Types of entity	SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory

VULNERABILITIES LINKED TO ATTACK METHOD 37 - ILLEGAL PROCESSING OF DATA

Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.38 ERROR IN USE

No explicit documentation on the application systems	
Types of entity	LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Users lack competency	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_INT: Communication interface MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No procedure for testing incoming goods and confirming their compliance with the specifications	
Types of entity	LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No validation of keyed data entries	
Types of entity	LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Lack of responsibility	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Application that is complex to use	

Types of entity	LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No accessible user support	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INF: Medium and supports MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Non-intuitive software	
Types of entity	LOG_OS: Operating system
Insufficient competency	
Types of entity	LOG_OS: Operating system
No accessible support	
Types of entity	LOG_OS: Operating system
No training in the use and maintenance of new software	
Types of entity	LOG_OS: Operating system
Software that is complex to use	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software
Equipment that is complex to use or not user-friendly	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment

	MAT_ACT.1: Transportable equipment MAT: Hardware
Incorrect operating conditions	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware
Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No labelling of media	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
Media are complex to use or not user-friendly	
Types of entity	MAT_PAS.1: Electronic medium
No monitoring of critical processes by the parent organisation	
Types of entity	ORG_DEP: Higher-tier organisation
No double checking of critical processes	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
No training on the equipment or software used	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Lack of understanding of responsibilities	
Types of entity	PER_DEC: Decision maker
No formalisation of responsibilities known by everyone	
Types of entity	PER_DEC: Decision maker
Unfavourable work conditions	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Lack of professionalism	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker

Failure to comply with instructions	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Users poorly trained or not trained at all	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Some highly sensitive operations can be performed by a single person	
Types of entity	PER_DEC: Decision maker
No user documentation for existing applications	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Lack of motivation for work involving data keying	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Personnel not used to keying	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Unfavourable work environment (rooms too small, lack of storage areas, etc.)	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No labelling of cables or cable layout plan	
Types of entity	PHY_SRV.1: Communication
Technical rooms too cramped	
Types of entity	PHY_SRV.1: Communication
No operating procedure	
Types of entity	PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power
No up-to-date labelling and diagram of the architecture	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
No cable layout plan	
Types of entity	RES_INF: Medium and supports
Interface with technical characteristics specific to the country (e.g. different telephone connectors between France and the United Kingdom)	
Types of entity	RES_INT: Communication interface
Medium and supports with technical characteristics specific to their locality (e.g.	

different ADSL configuration parameters between France and the United Kingdom)	
Types of entity	RES_REL: Passive or active relay
No protection measures (read only, etc.)	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
No supervision tool	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
VULNERABILITIES LINKED TO ATTACK METHOD 38 - ERROR IN USE	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral

	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.39 ABUSE OF RIGHTS

No audit policy	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No back-up of event logs	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No event logging	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
Assignment files too complex or unpractical	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system

Connection passwords not sufficiently complex	
Types of entity	LOG_OS: Operating system
Possibility of remote administration of the system using non-encrypted administration tools	
Types of entity	LOG_OS: Operating system
The password base of the operating system is decipherable	
Types of entity	LOG_OS: Operating system
The SNMP layer is activated	
Types of entity	LOG_OS: Operating system
Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	
Types of entity	LOG_STD: Package software or standard software LOG_OS: Operating system
The remote maintenance link is permanently activated	
Types of entity	LOG_OS: Operating system
Possibility of remote system administration	
Types of entity	LOG_OS: Operating system
The operating system logs can be modified by anyone	
Types of entity	LOG_OS: Operating system
Resource sharing makes it easy for unauthorised persons to use the system	
Types of entity	LOG_OS: Operating system
The operating system can be accessed and used by everyone (e.g. connection via the guest account)	
Types of entity	LOG_OS: Operating system
The operating system does not log system records or events	
Types of entity	LOG_OS: Operating system
The operating system can be used to make anonymous connections	
Types of entity	LOG_OS: Operating system
The operating system allows a session to be opened without password	
Types of entity	LOG_OS: Operating system
Possibility of remote system administration from any station	
Types of entity	LOG_OS: Operating system
Use of an obsolete version of the operating system or applications	
Types of entity	LOG_OS: Operating system
The passwords entered for access to the operating system are decipherable	
Types of entity	LOG_OS: Operating system
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	
Types of entity	LOG_OS: Operating system
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	

Types of entity	LOG_SRV: Service, maintenance or administration software
No physical protection	
Types of entity	MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No robust access control system	
Types of entity	MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No audit of physical access control procedures	
Types of entity	MAT_PAS.2: Other media
No authorisation management and monitoring policy imposed at the organisation's sites	
Types of entity	ORG_DEP: Higher-tier organisation
Responsibilities for information systems security not dealt with in the internal regulations	
Types of entity	ORG_DEP: Higher-tier organisation
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clauses setting out the responsibilities of both parties	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No definition of the right to know	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No provisions for monitoring and sanctioning	
Types of entity	ORG_GEN: Structure of the organisation
No regulation defining rights	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Assignment of user rights is not clearly defined	
Types of entity	ORG_GEN: Structure of the organisation
User grant rights are not controlled.	
Types of entity	ORG_PRO: Project or system organisation
Personnel categories with higher access privileges	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer

	PER_DEC: Decision maker PER: Personnel
Some highly sensitive operations can be performed by a single person	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
The notion of right is not defined for the personnel	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No procedures for checking authorisation of personnel entering the site or the premises	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No physical and logical protection	
Types of entity	RES_INF: Medium and supports
The principle of least privilege is not applied	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface
Resources can be used without tracking	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The system can be accessed by everyone	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
VULNERABILITIES LINKED TO ATTACK METHOD 39 - ABUSE OF RIGHTS	

Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.40 FORGING OF RIGHTS

No audit policy	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory

	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No back-up of event logs	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No event logging	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
The operating system logs can be modified by anyone	
Types of entity	LOG_OS: Operating system
The operating system allows a session to be opened without password	
Types of entity	LOG_OS: Operating system
The operating system can be used to make anonymous connections	
Types of entity	LOG_OS: Operating system
The operating system does not log system records or events	
Types of entity	LOG_OS: Operating system
The operating system can be accessed and used by everyone (e.g. connection via the guest account)	
Types of entity	LOG_OS: Operating system
Resource sharing makes it easy for unauthorised persons to use the system	
Types of entity	LOG_OS: Operating system
The password base of the operating system is decipherable	
Types of entity	LOG_OS: Operating system
The SNMP layer is activated	
Types of entity	SYS_MES: Electronic messaging LOG_OS: Operating system
Assignment files too complex or unpractical	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface

	LOG_OS: Operating system
Possibility of remote administration of the system using non-encrypted administration tools	
Types of entity	SYS_MES: Electronic messaging LOG_OS: Operating system
Possibility of remote system administration	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
The remote maintenance link is permanently activated	
Types of entity	SYS_MES: Electronic messaging RES_REL: Passive or active relay RES_INT: Communication interface LOG_OS: Operating system
The passwords entered for access to the operating system are decipherable	
Types of entity	LOG_OS: Operating system
Connection passwords not sufficiently complex	
Types of entity	SYS_MES: Electronic messaging LOG_OS: Operating system
Use of an obsolete version of the operating system or applications	
Types of entity	SYS_MES: Electronic messaging LOG_OS: Operating system
Possibility of the system being subjected to badly formed requests and data (e.g. buffer overflow)	
Types of entity	LOG_STD: Package software or standard software LOG_OS: Operating system
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	
Types of entity	LOG_OS: Operating system
Possibility of remote system administration from any station	
Types of entity	SYS_MES: Electronic messaging LOG_OS: Operating system
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	
Types of entity	LOG_SRV: Service, maintenance or administration software
The equipment is connected to external networks	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No robust access control system	
Types of entity	RES_REL: Passive or active relay MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment

No partitioning of equipment	
Types of entity	MAT_ACT.3: Processing peripheral
No protection of media	
Types of entity	MAT_PAS.1: Electronic medium
No audit of physical access control procedures	
Types of entity	MAT_PAS.2: Other media
Managers have no contact with the expertise or technology watch departments	
Types of entity	ORG_DEP: Higher-tier organisation
No rules and procedures for personnel authorisation	
Types of entity	ORG_DEP: Higher-tier organisation
No awareness of the risks of sanction	
Types of entity	ORG_DEP: Higher-tier organisation
Responsibilities for information systems security not dealt with in the internal regulations	
Types of entity	ORG_DEP: Higher-tier organisation
No monitoring procedure	
Types of entity	ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
Possibility of using the organisation's resources without supervision (self-service equipment, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
No protection of spaces dedicated to information exchange or sharing	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No procedure for personnel authorisation	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
No climate of trust between individuals	
Types of entity	ORG_PRO: Project or system organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers
The security responsibilities concerning authorisation management are not formalised.	
Types of entity	ORG_GEN: Structure of the organisation
Personnel receive no communication or information concerning authorisation procedures	
Types of entity	ORG_GEN: Structure of the organisation
No procedure for passing up information in the event of detection	
Types of entity	ORG_GEN: Structure of the organisation
The security policy is not applied	
Types of entity	ORG_GEN: Structure of the organisation

Inappropriate organisation	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Rights assigned without legitimate need	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Conflictual situation between persons	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No code of conduct	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Some highly sensitive operations can be performed by a single person	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Missions not suited to the personnel	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance

	PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
No procedures for checking authorisation of personnel entering the site or the premises	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
No physical and logical protection (partitioning, etc.)	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network
No network partitioning	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
The interfaces are connected to external networks	
Types of entity	RES_INF: Medium and supports
The supports and medium are connected to external networks	
Types of entity	RES_INF: Medium and supports
Technical characteristics can be modified (e.g. MAC address of an Ethernet card)	
Types of entity	RES_INF: Medium and supports
No physical protection	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
The network allows the system resources to be modified or adjusted	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
Presence of protocol that has no authentication function	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The interfaces can be accessed by everyone	
Types of entity	RES_INT: Communication interface
The network makes it easy for unauthorised persons to use the resources	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)	
Types of entity	RES_REL: Passive or active relay
The system can be accessed by everyone	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device

	SYS_ANU: Company directory
Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	
Types of entity	SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory
Applications are not checked before installation	
Types of entity	SYS_MES: Electronic messaging
The messaging system can be accessed from Internet	
Types of entity	SYS_MES: Electronic messaging
Use of an obsolete version of the messaging server	
Types of entity	SYS_MES: Electronic messaging
VULNERABILITIES LINKED TO ATTACK METHOD 40 - USURPING OF RIGHT	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment

	MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.41 DENIAL OF ACTIONS

No audit policy	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software
No back-up of event logs	
Types of entity	LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
No event logging	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application
The operating system does not log system records or events	
Types of entity	LOG_OS: Operating system
The SNMP layer is activated	
Types of entity	LOG_OS: Operating system
Possibility of remote administration of the system using non-encrypted administration tools	

Types of entity	LOG_OS: Operating system
Assignment files too complex or unpractical	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports LOG_OS: Operating system
Connection passwords not sufficiently complex	
Types of entity	LOG_OS: Operating system
The passwords entered for access to the operating system are decipherable	
Types of entity	LOG_OS: Operating system
The password base of the operating system is decipherable	
Types of entity	LOG_OS: Operating system
The operating system can be used to make anonymous connections	
Types of entity	LOG_OS: Operating system
Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	
Types of entity	LOG_STD: Package software or standard software LOG_OS: Operating system
Possibility of remote system administration from any station	
Types of entity	LOG_OS: Operating system
Use of an obsolete version of the operating system or applications	
Types of entity	LOG_OS: Operating system
The operating system can be accessed and used by everyone (e.g. connection via the guest account)	
Types of entity	LOG_OS: Operating system
Possibility of remote system administration	
Types of entity	LOG_OS: Operating system
The operating system logs can be modified by anyone	
Types of entity	LOG_OS: Operating system
Possibility of booting several operating systems on the same machine (e.g. access to NTFS partitions via Linux)	
Types of entity	LOG_OS: Operating system
The operating system allows a session to be opened without password	
Types of entity	LOG_OS: Operating system
The remote maintenance link is permanently activated	
Types of entity	LOG_OS: Operating system
Resource sharing makes it easy for unauthorised persons to use the system	
Types of entity	LOG_OS: Operating system
Software can be used by everyone (e.g. no password required for remote administration of a workstation)	
Types of entity	LOG_SRV: Service, maintenance or administration software
No tracking and auditing system	

Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
The equipment can be accessed and used by everyone	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
Media available to everyone	
Types of entity	MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
No procedure for access to classified information	
Types of entity	MAT_PAS.2: Other media
Change of the organisation's policy or strategy	
Types of entity	PER_UTI: Users PER_DEC: Decision maker ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No definition of responsibilities	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
Responsibilities for information systems security not dealt with in the internal regulations	
Types of entity	ORG_DEP: Higher-tier organisation
No disciplinary procedures	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
High political / economic stakes	
Types of entity	ORG_DEP: Higher-tier organisation
No global policy for managing and archiving tracks and other elements of proof	
Types of entity	ORG_DEP: Higher-tier organisation
No contractual clause concerning the definition of communication and exchange procedures	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No mutual checking of codes	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
Penalty or sanction clause out of proportion or not suited to the context	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No mechanism for monitoring actions, logs and alerts	

Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
Possibility of using the organisation's resources without supervision (self-service equipment, etc.)	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No hierarchical organisation or reporting procedure	
Types of entity	ORG_PRO: Project or system organisation
Audit functions are not separate from monitoring functions	
Types of entity	ORG_PRO: Project or system organisation
No management support for application of the security policy	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel
Obtaining an advantage	
Types of entity	PER_UTI: Users PER_DEC: Decision maker
Lack of confidence in the organisation	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Responsibility of each person not known	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
Conflictual situation between persons	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker
No history recording persons entering and leaving	
Types of entity	PHY_LIE.3: Zone PHY_LIE.2: Premises
The relays can be accessed by everyone	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
The medium allows system resources to be used from outside	
Types of entity	RES_INF: Medium and supports
The supports and medium can be accessed by everyone and are active by default (e.g. RJ45 connectors intermingled)	

Types of entity	RES_INF: Medium and supports
The network makes it easy for unauthorised persons to use the resources	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The protocol does not allow certain identification of the sender	
Types of entity	RES_INT: Communication interface
The network allows the system resources to be modified or adjusted	
Types of entity	RES_REL: Passive or active relay RES_INT: Communication interface
The protocol does not allow acknowledgement of receipt to be sent	
Types of entity	RES_INT: Communication interface
Resources can be used without tracking	
Types of entity	RES_INT: Communication interface
The access system does not log tracks of its operation	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
Access to the tracking system is not protected	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The system can be accessed by everyone (e.g. does not authenticate client stations or users)	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
The system is connected to external networks	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System
VULNERABILITIES LINKED TO ATTACK METHOD 41 - DENIAL OF ACTIONS	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging

	SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

4.42 BREACH OF PERSONNEL AVAILABILITY

Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	
Types of entity	MAT_ACT: Data processing equipment (active) MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment
No archiving procedure	
Types of entity	MAT_PAS: Data medium (passive)

	MAT_PAS.2: Other media MAT_PAS.1: Electronic medium
Unfavourable industrial relations	
Types of entity	ORG_DEP: Higher-tier organisation
Political / economic conflict between the organisation's home country and its host country	
Types of entity	ORG_GEN: Structure of the organisation ORG_DEP: Higher-tier organisation
No clause or procedures for transfer of knowledge	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
The organisation's financial or technological continuity is not secure	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No continuity clause for service provision	
Types of entity	ORG_EXT: Subcontractors / Suppliers / Manufacturers
No personnel protection team	
Types of entity	ORG_GEN: Structure of the organisation
Viral epidemic in the locality	
Types of entity	ORG_GEN: Structure of the organisation
No procedures for transfer of knowledge	
Types of entity	PER_UTI: Users ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
The organisation's activity is impaired by its industrial relations	
Types of entity	ORG_GEN: Structure of the organisation
No awareness and training programme for processes relating to continuity of professional activities	
Types of entity	ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation
No process for managing the continuity of the organisation's professional activities	
Types of entity	ORG_GEN: Structure of the organisation
The organisation is under-sized	
Types of entity	ORG_PRO: Project or system organisation
No substitutes for strategic personnel	
Types of entity	ORG_PRO: Project or system organisation
No substitute organisation for sensitive functions	
Types of entity	ORG_PRO: Project or system organisation
No process for managing the continuity of the project team's professional activities	
Types of entity	ORG_PRO: Project or system organisation
No document base for rules and procedures	
Types of entity	ORG_PRO: Project or system organisation
Unavailability arising from a competition factor	

Types of entity	PER_DEC: Decision maker
Unavailability caused by illness	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Unavailability caused by absenteeism	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Unavailability caused by third parties (physical aggression, hostage taking, etc.)	
Types of entity	PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer
Social problems	
Types of entity	PER_EXP: Operator / Maintenance PER_DEV: Developer
Conflictual industrial relations	
Types of entity	PER_UTI: Users
Difficult industrial relations possibly resulting in transport strikes	
Types of entity	PHY_LIE.1: External environment
Specialised personnel accommodated in remote rooms	
Types of entity	PHY_LIE.2: Premises
Personnel living a long way from the premises	
Types of entity	PHY_LIE.2: Premises
Possible harm to personnel using the equipment (wireless transmission, emanations, etc.)	
Types of entity	RES_REL: Passive or active relay RES_INF: Medium and supports
VULNERABILITIES LINKED TO ATTACK METHOD 42 - BREACH OF PERSONNEL AVAILABILITY	
Types of entity	SYS_WEB: External portal SYS_MES: Electronic messaging SYS_ITR: Intranet SYS_INT: Internet access device SYS_ANU: Company directory SYS: System RES_REL: Passive or active relay RES_INT: Communication interface RES_INF: Medium and supports RES: Network PHY_SRV: Essential service PHY_SRV.3: Cooling / pollution PHY_SRV.2: Power PHY_SRV.1: Communication PHY_LIE: Places

	PHY_LIE.3: Zone PHY_LIE.2: Premises PHY_LIE.1: External environment PER_UTI: Users PER_EXP: Operator / Maintenance PER_DEV: Developer PER_DEC: Decision maker PER: Personnel ORG_PRO: Project or system organisation ORG_GEN: Structure of the organisation ORG_EXT: Subcontractors / Suppliers / Manufacturers ORG_DEP: Higher-tier organisation ORG: Organisation MAT_PAS: Data medium (passive) MAT_PAS.2: Other media MAT_PAS.1: Electronic medium MAT_ACT: Data processing equipment (active) MAT_ACT.3: Processing peripheral MAT_ACT.2: Fixed equipment MAT_ACT.1: Transportable equipment MAT: Hardware LOG_STD: Package software or standard software LOG_SRV: Service, maintenance or administration software LOG_OS: Operating system LOG_APP: Business application LOG_APP.2: Specific business application LOG_APP.1: Standard business application LOG: Software

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