

Annex C – EXAMPLES

C.1 ASSET TYPES

<p>MAT: Hardware</p> <p>Description – The hardware type consists of all the physical elements of an information system.</p>	<p>MAT_ACT: Data processing equipment (active)</p> <p>Description – Automatic information processing equipment including the items it requires to operate independently.</p>	<p>MAT_ACT.1: Transportable equipment</p> <p>Description – Computer equipment designed to be carried by hand and used in different places.</p> <p>Examples – Laptop computer, PDA.</p>
		<p>MAT_ACT.2: Fixed equipment</p> <p>Description – Computer equipment belonging to the organisation or used in the organisation’s premises.</p> <p>Examples – Server, microcomputer used as a workstation.</p>
		<p>MAT_ACT.3: Processing peripheral</p> <p>Description – Equipment connected to a computer via a communication port (serial, parallel link, etc.) for entering, conveying or transmitting data.</p> <p>Examples – Printer, removable disc drive.</p>
	<p>MAT_PAS: Data medium (passive)</p> <p>Description – These are media for storing data or functions.</p>	<p>MAT_PAS.1: Electronic medium</p> <p>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.</p> <p>Examples – Floppy disc, CD ROM, back-up cartridge, removable hard disc, memory key, tape.</p>

ANNEX C – EXAMPLES

		<p>MAT_PAS.2: Other media</p> <p>Description – Static, non-electronic media containing data.</p> <p>Examples – Paper, slide, transparency, documentation, fax.</p>
<p>LOG: Software</p> <p>Description – The software type consists of all the programmes contributing to the operation of a data processing set.</p>	<p>LOG_OS: Operating system</p> <p>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.</p> <p>Examples – GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS.</p>	

	<p>LOG_SRV: Service, maintenance or administration software</p> <p>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).</p> <p>Examples – GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS.</p>	
	<p>LOG_STD: Package software or standard software</p> <p>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.</p> <p>Examples – Data base management software, electronic messaging software, groupware, directory software, Webserver software, etc. (Oracle, DB2, IIS, Apache, Lotus Notes, Exchange, OpenLDAP, etc.).</p>	

ANNEX C – EXAMPLES

	LOG_APP: Business application	<p>LOG_APP.1: Standard business application</p> <p>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.</p> <p>Examples – Accounts software, machine tool control software, customer care software, personnel competency management software, administrative teleprocedure software, etc.</p>
		<p>LOG_APP.2: Specific business application</p> <p>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.</p> <p>Examples – Invoice management of telecom operators’ customers, real time monitoring application for rocket launching.</p>

<p>RES: Network</p> <p>Description – The network type consists of all telecommunications devices used to interconnect several physically remote computers or components of an information system.</p>	<p>RES_INF: Medium and supports</p> <p>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).</p> <p>Examples – PSTN, Ethernet, GigabitEthernet, cable, fibre, copper ADSL, WiFi 802.11, BlueTooth, FireWire.</p>	
	<p>RES_REL: Passive or active relay</p> <p>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.</p> <p>Examples – Bridge, router, hub, switch, automatic exchange.</p>	

ANNEX C – EXAMPLES

	<p>RES_INT: Communication interface</p> <p>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.</p> <p>Examples – Wifi, GPRS, Ethernet adaptor.</p>	
<p>PER: Personnel</p> <p>Description – The personnel type consists of all the groups of persons involved in the information system.</p>	<p>PER_DEC: Decision maker</p> <p>Description – Decision makers are the owners of the essential elements (information and functions) and the line managers of the organisation or specific project.</p> <p>Examples – Top management, Project leader.</p>	
	<p>PER_UTI: Users</p> <p>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.</p>	

	<p>PER_EXP: Operator / Maintenance</p> <p>Description – These are the personnel in charge of operating and maintaining the information system. They have special access rights to the information system to carry out their everyday tasks.</p> <p>Examples – System administrator, data administrator, back-up, Help Desk, application deployment operator, security officers.</p>	
	<p>PER_DEV: Developer</p> <p>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.</p> <p>Examples – Business application developers.</p>	
<p>PHY: Site</p> <p>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.</p>	<p>PHY_LIE: Places</p> <p>Description – Perimeters, physical enclosures.</p>	<p>PHY_LIE.1: External environment</p> <p>Description – This concerns all the places in which the organisation’s means of security cannot be applied.</p> <p>Examples – Homes of the personnel, premises of another organisation, environment outside the site (urban area, hazard area).</p>

ANNEX C – EXAMPLES

		<p>PHY_LIE.2: Premises</p> <p>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.</p> <p>Examples – Establishment, buildings.</p>
		<p>PHY_LIE.3: Zone</p> <p>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.</p> <p>Examples – Offices, reserved access zone, secure zone.</p>
	<p>PHY_SRV: Essential service</p> <p>Description – All the services required for the organisation’s equipment to operate.</p>	<p>PHY_SRV.1: Communication</p> <p>Description – Telecommunications services and equipment provided by an operator.</p> <p>Examples – Telephone line, PABX, internal telephone networks.</p>
		<p>PHY_SRV.2: Power</p> <p>Description – Services and means (sources and wiring) required for providing power to information technology equipment and peripherals.</p> <p>Examples – Low voltage power supply, inverter, electrical circuit head-end.</p>

		<p>PHY_SRV.3: Cooling / pollution</p> <p>Description – Services and means (equipment, control) for cooling and purifying the air.</p> <p>Examples – Chilled water pipes, air-conditioners.</p>
<p>ORG: Organisation</p> <p>Description – The organisation type describes the organisational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.</p>	<p>ORG_DEP: Higher-tier organisation</p> <p>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.</p> <p>Examples – Administrating body, head office of an organisation, court of auditors.</p>	
	<p>ORG_GEN: Structure of the organisation</p> <p>Description – This consists of the various branches of the organisation, including its cross-functional activities, under the control of its management.</p> <p>Examples – Human resources management, IT management, purchasing management, business unit management, building safety service, fire service, audit management.</p>	

ANNEX C – EXAMPLES

	<p>ORG_PRO: Project or system organisation</p> <p>Description – This concerns the organisation set up for a specific project or service.</p> <p>Examples – New application development project, information system migration project.</p>	
	<p>ORG_EXT: Subcontractors / Suppliers / Manufacturers</p> <p>Description – An organisation providing the organisation with a service or resources and bound to it by contract.</p> <p>Examples – Facilities management company, outsourcing company, consultancy companies.</p>	
<p>SYS: System</p> <p>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.</p>	<p>SYS_INT: Internet access device</p> <p>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.</p> <p>Examples – Filtering device, DMZ, gateways.</p>	
	<p>SYS_MES: Electronic messaging</p> <p>Description – A device allowing authorised users to type, query and send computerised documents or electronic messages from or to computers connected in network.</p> <p>Examples – Internal electronic mail, Web electronic mail.</p>	

	<p>SYS_ITR: Intranet</p> <p>Description – Shared and private data and information services, using communication protocols and core technologies (Internet technology for example).</p> <p>Examples – Internal information system.</p>	
	<p>SYS_ANU: Company directory</p> <p>Description – A device for managing and accessing a data base describing the company’s personnel and their characteristics.</p> <p>Examples – Management of application rights.</p>	
	<p>SYS_WEB: External portal</p> <p>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.</p> <p>Examples – Information portal, teleprocedure portal, electronic business site.</p>	

C.2 THREATS DESCRIPTION

The **Description** can include:

- Category
- Attack method
- Concerned security needs (CIA)
- Associated assets types
- Difficulty (cost, time, physical access, ...)
- Type: human, physical, environmental

Threats can be described with different level of refinement.

C.3 VULNERABILITIES DESCRIPTION

A common vulnerability format **Description** should be set up. This has to be linked with the NCIRC: NATO Computer Incident response capability.

Name

Entities

Attack method

Type: technical, environment, procedures cf D1020

Technical:

Protocols

Software products:

Operating systems:

Windows

UNIX

LINUX

Application software:

Office suite

Message handling system

Databases

Web servers

Specific software

Hardware products:

PC

Network Switches

Routers

Firewalls

Mainframes

Printers

Cryptographic algorithm