**Annex B**

(informative)

## Identification and valuation of assets and impact assessment

### B.1 Examples of asset identification

To perform asset valuation, an organization first needs to identify its assets(at an appropriate level of detail). Two kinds of assets can be distinguished:

* The primary assets:
* Business processes & activities
* Information
* The supporting assets (on which the primary elements of the scope rely) of all types:
* Hardware
* Software
* Network
* Personnel
* Site
* Organization’s structure

#### **B.1.1 The identification of primary assets**

To describe the scope more accurately, this activity consists in identifying the primary assets (business processes and activities, information). This identification is carried out by a mixed work group representative of the process (managers, information systems specialists and users).

The primary assets are usually the core processes and information of the activity in the scope. Other primary assets such as the organization's processes can also be considered, which will be more appropriate for drawing up an information security policy or a business continuity plan. Depending on the purpose, some studies will not require an exhaustive analysis of all the elements making up the scope. In such cases, the study boundaries can be limited to the key elements of the scope.

Primary assets are of two types:

1 - Business processes (or sub-processes) and activities, for example:

* Processes whose loss or degradation make it impossible to carry out the mission of the organization
* Processes that contain secret processes or processes involving proprietary technology
* Processes that, if modified, can greatly affect the accomplishment of the organization's mission
* Processes that are necessary for the organization to comply with contractual, legal or regulatory requirements

2 – Information:

More generally, primary information mainly comprises:

* Vital information for the exercise of the organization's mission or business
* Personal information, as can be defined specifically in the sense of the national laws regarding privacy
* Strategic information required for achieving objectives determined by the strategic orientations
* High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

Processes and information that are not identified as sensitive after this activity will have no defined classification in the remainder of the study. This means that even if such processes or information are compromised, the organization will still accomplish the mission successfully.

However, they will often inherit controls implemented to protect the processes and information identified as sensitive.

#### **B.1.2 List and description of supporting assets**

The scope consists of assets that should be identified and described. These assets have vulnerabilities that are exploitable by threats aiming to impair the primary assets of the scope (processes and information). They are of various types:

Hardware

The hardware type consists of all the physical elements supporting processes.

##### Data processing equipment (active)

Automatic information processing equipment including the items required to operate independently. Transportable equipment

Portable computer equipment.

Examples: laptop computer, Personal Digital Assistant (PDA).

##### Fixed equipment

Computer equipment used on the organization's premises.

Examples: server, microcomputer used as a workstation.

##### Processing peripherals

Equipment connected to a computer via a communication port (serial, parallel link, etc.) for entering, conveying or transmitting data.

Examples: printer, removable disc drive.

Data medium (passive)

These are media for storing data or functions.

##### Electronic medium

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.

##### Other media

Static, non-electronic media containing data.

Examples: paper, slide, transparency, documentation, fax.

Software

Software consists of all the programmes contributing to the operation of a data processing set.

##### Operating system

This 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 elements of the operating system are all the equipment management services (CPU, memory, disc, and network interfaces), task or process management services and user rights management services.

##### Service, maintenance or administration software

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).

##### Package software or standard software

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 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, web server software, etc.

Business application

##### Standard business application

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 software, etc.

##### Specific business application

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. There is a very wide, theoretically unlimited, range of fields.

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

##### Network

The network type consists of all telecommunications devices used to interconnect several physically remote computers or elements of an information system.

##### Medium and supports

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: Public Switching Telephone Network (PSTN), Ethernet, GigabitEthernet, Asymmetric Digital Subscriber Line (ADSL), wireless protocol specifications (e.g. WiFi 802.11), Bluetooth, FireWire.

##### Passive or active relay

This sub-type includes all devices that are not the logical terminations of communications (IS vision) but are intermediate or relay devices. Relays 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 usually capable of generating logs.

Examples: bridge, router, hub, switch, automatic exchange.

##### Communication interface

The communication interfaces of the processing units 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: General Packet Radio Service (GPRS), Ethernet adaptor.

Personnel

The personnel type consists of all the groups of people involved in the information system.

##### Decision maker

Decision makers are the owners of the primary assets (information and functions) and the managers of the organization or specific project.

Examples: top management, project leader.

##### Users

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.

##### Operation/ Maintenance staff

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.

Examples: system administrator, data administrator, back-up, Help Desk, application deployment operator, security officers.

##### Developers

Developers are in charge of developing the organization'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.

##### Site

The site type comprises all the places containing the scope or part of the scope, and the physical means required for it to operate.

Location

##### External environment

This concerns all locations in which the organization's means of security cannot be applied.

Examples: homes of the personnel, premises of another organization, environment outside the site (urban area, hazard area).

##### Premises

This place is bounded by the organization'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.

##### Zone

A zone is formed by a physical protective boundary forming partitions within the organization's premises. It is obtained by creating physical barriers around the organization's information processing infrastructures.

Examples: offices, reserved access zone, secure zone.

Essential services

All the services required for the organization's equipment to operate.

##### Communication

Telecommunications services and equipment provided by an operator.

Examples: telephone line, PABX, internal telephone networks.

##### Utilities

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.

Water supply

Waste disposal

Services and means (equipment, control) for cooling and purifying the air.

Examples: chilled water pipes, air-conditioners.

##### Organization

The organization type describes the organizational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

##### Authorities

These are organizations from which the studied organization derives its authority. They may be legally affiliated or external. This imposes constraints on the studied organization in terms of regulations, decisions and actions.

Examples: administrating body, Head office of an organization.

##### Structure of the organization

This consists of the various branches of the organization, 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.

##### Project or system organization

This concerns the organization set up for a specific project or service.

Examples: new application development project, information system migration project.

##### Subcontractors / Suppliers / Manufacturers

These are organizations that provide the organization with a service or resources and bound to it by contract.

Examples: facilities management company, outsourcing company, consultancy companies.

### B.2 Asset valuation

The next step after asset identification is to agree upon the scale to be used and the criteria for assigning a particular location on that scale to each asset, based on valuation. Because of the diversity of assets found within most organizations it is likely that some assets that have a known monetary value will be valued in the local unit of currency while others which have a more qualitative value may be assigned a value ranging, for example, from ”very low” to ”very high”. The decision to use a quantitative scale versus a qualitative scale is really a matter of organizational preference, but should be relevant to the assets being valued. Both valuation types could be used for the same asset.

Typical terms used for the qualitative valuation of assets include words such as: negligible, very low, low, medium, high, very high, and critical. The choice and range of terms suitable to an organization is strongly dependent on an organization's needs for security, organizational size, and other organization specific factors.

#### Criteria

The criteria used as the basis for assigning a value to each asset should be written out in unambiguous terms. This is often one of the most difficult aspects of asset valuation since the values of some assets may have to be subjectively determined and since many different individuals are likely to be making the determination. Possible criteria used to determine an asset’s value include its original cost, its replacement or re-creation cost or its value may be abstract, e.g. the value of an organization’s reputation.

Another basis for the valuation of assets is the costs incurred due to the loss of confidentiality, integrity and availability as the result of an incident. Non-repudiation, accountability, authenticity and reliability should also be considered, as appropriate. Such a valuation would provide the important element dimensions to asset value, in addition to replacement cost, based on estimates of the adverse business consequences that would result from security incidents with an assumed set of circumstances. It is emphasized that this approach accounts for consequences that are necessary to factor into the risk assessment.

Many assets may during the course of valuation have several values assigned. For example: a business plan may be valued based on the labour expended to develop the plan, it might be valued on the labour to input the data, and it could be valued based on its value to a competitor. Each of the assigned values will most likely differ considerably. The assigned value may be the maximum of all possible values or may be the sum of some or all of the possible values. In the final analysis, which value or values are assigned to an asset should be carefully determined since the final value assigned enters into the determination of the resources to be expended for the protection of the asset.

#### Reduction to the common base

Ultimately, all asset valuations need to be reduced to a common base. This may be done with the aid of criteria such as those that follow. Criteria that may be used to assess the possible consequences resulting from a loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, or reliability of assets are:

* Violation of legislation and/or regulation
* Impairment of business performance
* Loss of goodwill/negative effect on reputation
* Breach associated with personal information
* Endangerment of personal safety
* Adverse effects on law enforcement
* Breach of confidentiality
* Breach of public order
* Financial loss
* Disruption to business activities
* Endangerment of environmental safety

Another approach to assess the consequences could be:

* Interruption of service
* inability to provide the service
* Loss of customer confidence
* loss of credibility in the internal information system
* damage to reputation
* Disruption of internal operation
* disruption in the organization itself
* additional internal cost  Disruption of a third party's operation:
* disruption in third parties transacting with the organization  various types of injury  Infringement of laws / regulations:
* inability to fulfill legal obligations  Breach of contract:
* inability to fulfill contractual obligations  Danger to personnel / user safety:
* danger for the organization's personnel and / or users
* Attack on users' private life
* Financial losses
* Financial costs for emergency or repair:
* in terms of personnel,
* in terms of equipment,
* in terms of studies, experts' reports
* Loss of goods / funds / assets
* Loss of customers, loss of suppliers
* Judicial proceedings and penalties
* Loss of a competitive advantage
* Loss of technological / technical lead
* Loss of effectiveness / trust
* Loss of technical reputation
* Weakening of negotiating capacity
* Industrial crisis (strikes)
* Government crisis
* Dismissal
* Material damage

These criteria are examples of issues to be considered for asset valuation. For carrying out valuations, an organization needs to select criteria relevant to its type of business and security requirements. This might mean that some of the criteria listed above are not applicable, and that others might need to be added to the list.

#### Scale

After establishing the criteria to be considered, the organization should agree on a scale to be used organization-wide. The first step is to decide on the number of levels to be used. There are no rules with regard to the number of levels that are most appropriate. More levels provide a greater level of granularity but sometimes a too fine differentiation makes consistent assignments throughout the organization difficult. Normally, any number of levels between 3 (e.g. low, medium, and high) and 10 can be used as long as it is consistent with the approach the organization is using for the whole risk assessment process.

An organization may define its own limits for asset values, like “low”, “medium”, or “high”. These limits should be assessed according to the criteria selected (e.g. for possible financial loss, they should be given in monetary values, but for considerations such as endangerment of personal safety, monetary valuation can be complex and may not be appropriate for all organizations). Finally, it is entirely up to the organization to decide what is considered as being “low” or a “high” consequence. A consequence that might be disastrous for a small organization could be low or even negligible for a very large organization.

#### Dependencies

The more relevant and numerous the business processes supported by an asset, the greater the value of this asset. Dependencies of assets on business processes and other assets should be identified as well since this might influence the values of the assets. For example, the confidentiality of data should be kept throughout its life-cycle, at all stages, including storage and processing, i.e. the security needs of data storage and processing programmes should be directly related to the value representing the confidentiality of the data stored and processed. Also, if a business process is relying on the integrity of certain data being produced by a programme, the input data of this programme should be of appropriate reliability. Moreover, the integrity of information will be dependent on the hardware and software used for its storage and processing. Also, the hardware will be dependent on the power supply and possibly air conditioning. Thus information about dependencies will assist in the identification of threats and particularly vulnerabilities. Additionally, it will help to assure that the true value of the assets (through the dependency relationships) is given to the assets, thereby indicating the appropriate level of protection.

The values of assets on which other assets are dependent may be modified in the following way:

* If the values of the dependent assets (e.g. data) are lower or equal to the value of the asset considered (e.g. software), its value remains the same
* If the values of the dependent asset (e.g. data) is greater, then the value of the asset considered (e.g.

software) should be increased according to:

* + The degree of dependency
  + The values of the other assets

An organization may have some assets that are available more than once, like copies of software programmes or the same type of computer used in most of the offices. It is important to consider this fact when doing the asset valuation. On one hand, these assets are overlooked easily, therefore care should be taken to identify all of them; on the other hand, they could be used to reduce availability problems.

#### Output

The final output of this step is a list of assets and their values relative to disclosure (preservation of confidentiality), modification (preservation of integrity, authenticity, non-repudiation and accountability), nonavailability and destruction (preservation of availability and reliability), and replacement cost.

### B.3 Impact assessment

An information security incident can impact more than one asset or only a part of an asset. Impact is related to the degree of success of the incident. As a consequence, there is an important difference between the asset value and the impact resulting from the incident. Impact is considered as having either an immediate (operational) effect or a future (business) effect that includes financial and market consequences.

Immediate (operational) impact is either direct or indirect.

Direct:

1. The financial replacement value of lost (part of) asset
2. The cost of acquisition, configuration and installation of the new asset or back-up
3. The cost of suspended operations due to the incident until the service provided by the asset(s) is restored d) Impact results in a information security breach

Indirect:

1. Opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere)
2. The cost of interrupted operations
3. Potential misuse of information obtained through a security breach
4. Violation of statutory or regulatory obligations
5. Violation of ethical codes of conduct

As such, the first assessment (with no controls of any kind) will estimate an impact as very close to the (combination of the) concerned asset value(s). For any next iteration for this (these) asset(s), the impact will be different (normally much lower) due to the presence and the effectiveness of the implemented controls.