**Annex A**

(informative)

## Defining the scope and boundaries of the information security risk management process

### A.1 Study of the organization

Evaluate the organization The study of the organization recalls the characteristic elements defining the identity of an organization. This concerns the purpose, business, missions, values and strategies of this organization. These should be identified together with the elements contributing to their development (e.g. subcontracting).

The difficulty of this activity lies in understanding exactly how the organization is structured. Identifying its real structure will provide an understanding of the role and importance of each division in achieving the organization's objectives.

*For example, the fact that the information security manager reports to the top managers rather than IT managers may indicate top managers' involvement in information security.*

The organization's main purpose The main purpose of an organization can be defined as the reason why it exists (its field of activity, its market segment, etc.).

Its business The organization's business, defined by the techniques and know-how of its employees, enables it to accomplish its missions. It is specific to the organization's field of activity and often defines its culture.

Its mission The organization achieves its purpose by accomplishing its mission. To identify its missions, the services provided and/or products manufactured should be identified in relation to the end users.

Its values Values are major principles or a well-defined code of conduct applied to the exercise of a business. This may concern the personnel, relations with outside agents (customers, etc.), the quality of products supplied or services provided.

*Take the example of an organization whose purpose is public service, whose business is transport and whose missions include transporting children to and from school. Its values may be the punctuality of the service and safety during transport.*

Structure of the organization There are different types of structure:

* Divisional structure: each division is placed under the authority of a division manager responsible for the strategic, administrative and operational decisions concerning his unit
* Functional structure: functional authority is exercised on the procedures, the nature of the work and sometimes the decisions or planning (e.g. production, IT, human resources, marketing, etc.)

Remarks:

* A division within an organization with divisional structure may be organised as a functional structure and vice versa
* An organization may be said to have a matrix structure if it has elements of both types of structure  In any organizational structure the following levels can be distinguished:
  + the decision-making level (definition of strategic orientations);
  + the leadership level (co-ordination and management);
  + the operational level (production and support activities).

Organization chart The organization's structure is represented schematically in an organization chart. This representation should highlight the lines of reporting and delegation of authority, but should also include other relationships, which, even if they are not based on any formal authority, are nevertheless lines of information flow.

The organization’s strategy This requires a formal expression of the organization's guiding principles. The organization’s strategy determines the direction and development needed in order to benefit from the issues at stake and of the major changes it is planning.

### A.2 List of the constraints affecting the organization

All the constraints affecting the organization and determining its information security orientation should be taken into account. Their source may be within the organization in which case it has some control over them or outside the organization and therefore generally non-negotiable. Resource constraints (budget, personnel) and emergency constraints are among the most important ones.

The organization sets its objectives (concerning its business, behaviour, etc.) committing it to a certain path, possibly over a long period. It defines what it wants to become and the means that will need to be implemented. In specifying this path, the organization takes into account developments in techniques and know-how, the expressed wishes of users, customers, etc. This objective can be expressed in the form of operating or development strategies with the aim, for example, of cutting operating costs, improving quality of service, etc.

These strategies probably include information and the information system (IS), which assist in their application. Consequently, characteristics concerning the identity, mission and strategies of the organization are fundamental elements in the analysis of the problem since the breach of an information security aspect could result in rethinking these strategic objectives. In addition, it is essential that proposals for information security requirements remain consistent with the rules, uses and means in force in the organization.

The list of constraints includes but is not limited to:

#### Constraints of a political nature

These may concern government administrations, public institutions or more generally any organization that has to apply government decisions. They are usually decisions concerning strategic or operational orientation made by a government division or decision-making body and should be applied.

*For example, the computerization of invoices or administrative documents introduces information security problems.*

#### Constraints of a strategic nature

Constraints can arise from planned or possible changes to the organization's structures or orientation. They are expressed in the organization's strategic or operational plans.

*For example, international co-operation in the sharing of sensitive information may necessitate agreements concerning secure exchange.*

#### Territorial constraints

The organization's structure and/or purpose may introduce specific constraints such as the distribution of sites over the entire national territory or abroad.

*Examples include postal services, embassies, banks, subsidiaries of a large industrial group, etc.*

#### Constraints arising from the economic and political climate

An organization's operation may be profoundly changed by specific events such as strikes or national and international crises.

*For example, some services should be able to continue even during a serious crisis.*

#### Structural constraints

The nature of an organization's structure (divisional, functional or other) may lead to a specific information security policy and security organization adapted to the structure.

*For example, an international structure should be able to reconcile security requirements specific to each country.*

#### Functional constraints

Functional constraints arise directly from the organization's general or specific missions.

*For example, an organization that operates around the clock should ensure its resources are continuously available.*

#### Constraints concerning personnel

The nature of these constraints varies considerably. They are linked to: level of responsibility, recruitment, qualification, training, security awareness, motivation, availability, etc.

*For example, the entire personnel of a defence organization should have authorisation to handle highly confidential information.*

#### Constraints arising from the organization's calendar

These constraints may result from restructuring or setting up new national or international policies imposing certain deadlines.

*For example, the creation of a security division.*

#### Constraints related to methods

Methods appropriate to the organization's know-how will need to be imposed for aspects such as project planning, specifications, development and so on.

*For example, a typical constraint of this kind is the need to incorporate the organization's legal obligations into the security policy.*

#### Constraints of a cultural nature

In some organizations work habits or the main business have led to a specific “culture” within the organization, one which may be incompatible with the security controls. This culture is the personnel's general reference framework and may be determined by many aspects, including education, instruction, professional experience, experience outside work, opinions, philosophy, beliefs, social status, etc.

#### Budgetary constraints

The recommended security controls may sometimes have a very high cost. While it is not always appropriate to base security investments on cost-effectiveness, economic justification is generally required by the organization’s financial department.

*For example, in the private sector and some public organizations, the total cost of security controls should not exceed the cost of the potential consequences of the risks. Top management should therefore assess and take calculated risks if they want to avoid excessive security costs.*

### A.3 List of the legislative and regulatory references applicable to the organization

The regulatory requirements applicable to the organization should be identified. These may be laws, decrees, specific regulations in the organization's field or internal and/or external regulations. This also concerns contracts and agreements and more generally any obligations of a legal or regulatory nature.

### A.4 List of the constraints affecting the scope

By identifying the constraints it is possible to list those that have an impact on the scope and determine which are nevertheless amenable to action. They are added to, and may possibly amend, the organization's constraints determined above. The following paragraphs present a non-exhaustive list of possible types of constraints.

#### Constraints arising from pre-existing processes

Application projects are not necessarily developed simultaneously. Some depend on pre-existing processes. Even though a process can be broken down into sub-processes, the process is not necessarily influenced by all the sub-processes of another process.

#### Technical constraints

Technical constraints, relating to infrastructure, generally arise from installed hardware and software, and rooms or sites housing the processes:

* Files (requirements concerning organization, media management, management of access rules, etc.)
* General architecture (requirements concerning topology (centralised, distributed, client-server), physical architecture, etc.)
* Application software (requirements concerning specific software design, market standards, etc.);
* Package software (requirements concerning standards, level of evaluation, quality, compliance with norms, security, etc.)
* Hardware (requirements concerning standards, quality, compliance with norms, etc.)
* Communication networks (requirements concerning coverage, standards, capacity, reliability, etc.)
* Building infrastructure (requirements concerning civil engineering, construction, high voltages, low voltages, etc.)

#### Financial constraints

The implementation of security controls is often restricted by the budget that the organization can commit. However, the financial constraint should still to be the last to be considered as the budget allocation for security can be negotiated on the basis of the security study.

#### Environmental constraints

Environmental constraints arise from the geographical or economic environment in which the processes are implemented: country, climate, natural risks, geographical situation, economic climate, etc.

#### Time constraints

The time required for implementing security controls should be considered in relation to the ability to upgrade the information system; if the implementation time is very long, the risks for which the control was designed may have changed. Time is a determining factor for selecting solutions and priorities.

#### Constraints related to methods

Methods appropriate to the organization's know-how should be used for project planning, specifications, development and so on.

#### Organizational constraints

Various constraints may follow from organizational requirements:

* Operation (requirements concerning lead-times, supply of services, surveillance, monitoring, emergency plans, degraded operation, etc.)
* Maintenance (requirements for incident troubleshooting, preventive actions, rapid correction, etc.)
* Human resources management (requirements concerning operator and user training, qualification for posts such as system administrator or data administrator, etc.)
* Administrative management (requirements concerning responsibilities, etc.)
* Development management (requirements concerning development tools, computer-aided software engineering, acceptance plans, organization to be set up, etc.)

Management of external relations (requirements concerning organization of third-party relations, contracts, etc.)