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 3
TECHNIQUES

Version 2 – 05 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
(see Comment Form at the end of the guide):

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 Guide to the Expression of Needs and Identification of Security Objectives (EBIOS).	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 scale of needs: 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 non-retained attack methods - 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 security functional requirements added to allow functional requirements covering security objectives to be determined and the extent of cover presented - Determination of security assurance requirements 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

SECTION 4 – TOOLS FOR ASSESSING ISS RISKS (separate document)

SECTION 5 – TOOLS FOR TREATING ISS RISKS (separate document)

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 third section of the method. It gives details of the method activities and proposes solutions for implementing them.

The techniques presented in this section are only proposals. Users of the document should choose the most appropriate techniques for their context, i.e. the culture and users in their organisation, as well as the tools they prefer to use. The level of detail can also be adjusted as necessary.

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

Step 1 - Context study

Activity 1.1 – Study of the organisation

Present the organisation

The presentation of the organisation recalls the characteristic elements defining the identity of an organisation. This concerns the purpose, business, missions, own values and lines of strategy of this organisation. These must be identified, together with the elements contributing to their development (e.g. subcontracting).

The difficulty of this activity lies in understanding exactly how the organisation is structured. Identifying its real structure will provide an understanding of the role and importance of each division in achieving the organisation's objectives.
For example, the fact that the security manager reports to top management rather than IT management may indicate top management's involvement in information systems security.

<u>The organisation's main purpose</u> (what it wants to do)

The main purpose of an organisation can be defined as the reason why it exists (its field of activity, its market segment, etc.). The purpose may, for example, be public service or industry.

<u>Its business</u> (what the organisation knows how to do)

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

<u>Its missions</u> (what the organisation must do)

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

<u>Its own values</u> (what the organisation does well)

"Own 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 organisation 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.

<u>Structure of the organisation</u>

There are different types of structure:

- ❑ divisional structure: each division is placed under the authority of a division director 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 organisation with divisional structure may be organised as a functional structure and vice versa;
- ❑ an organisation is said to have a matrix structure if it has elements of both types of structure;

- in any organisational 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).

Organisation chart

The organisation's structure is represented schematically in an organisation chart. This representation must 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.
For example, the IT correspondent who, as a user, is answerable to his head of department, may also receive instructions from IT management.

The lines of strategy (what the organisation wants to do better)

This requires a formal expression of the organisation's guiding principles, which determine the development needed in order to benefit from the issues at stake, and of the major changes it is planning.

List the constraints affecting the organisation.

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

The organisation sets itself objectives (concerning its business, behaviour, etc.) committing it to a certain path over a possibly long period. It defines what it wants to become and the means that will need to be implemented. In specifying this path, the organisation 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 policies, with the aim, for example, of cutting operating costs, improving quality of service, etc.

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

The following paragraphs present a non-exhaustive list of constraint types.

Constraints of a political nature

These may concern government administrations, public institutions or more generally any organisation that has to apply government decisions. They are usually decisions concerning strategic or operational orientation decisions made by a government division or decision-making body and must be applied.
For example, the computerisation of invoices or administrative documents introduces security problems.

Constraints of a strategic nature

Constraints can arise from planned or possible changes to the organisation's structures or orientations. They are expressed in the organisation's strategic or operational master plans.
For example, international co-operation in the sharing of sensitive information may necessitate agreements concerning secure exchange.

Territorial constraints

The organisation'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 climate

An organisation's operation may be profoundly changed by specific events such as strikes or national and international crises.
Some services must be able to continue even during serious crises.

Structural constraints

The nature of an organisation's structure (divisional, functional or other) may lead to a specific security policy and security organisation adapted to the structure.
For example, an international structure must be able to reconcile security requirements specific to each country.

Functional constraints

Functional constraints arise directly from the organisation's general or specific missions.
For example, an organisation that operates around the clock must ensure its means are permanently 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 organisation must have authorisation to handle highly confidential information.

Constraints arising from the organisation's calendar

These constraints may result from restructuring or setting up of new national or international policies imposing certain deadlines.
For example, the creation of a security division.

Constraints related to methods

Methods appropriate to the organisation's know-how will need to be imposed for aspects such as project planning, specifications, development and so on.
A typical constraint of this kind is the need to incorporate the organisation's quality actions into the security policy.

Constraints of a cultural nature

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

Budgetary constraints

The recommended security measures may sometimes have a very high cost. Even though it is inappropriate to base security investments on cost-effectiveness, some kind of economic justification is generally required by the organisation's financial departments.
For example, in the private sector and some public organisations, the total cost of security measures must not exceed the cost of the potential consequences of the feared risks. Top management must therefore assess and take calculated risks if it wants to avoid excessive security costs.

List the regulatory references applicable to the organisation.

Compliance with laws, rules or regulations may modify the environment, work habits, accomplishment of missions or have an influence on internal organisation.
For example, the operation of government administrations is controlled by specific regulations (customs regulations, public contract regulations, etc.).

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

Produce a functional description of the global IS

This involves identifying the functional domains that contribute to achieving the strategic objectives and their interactions. At this level every effort is made to represent the existing and/or future interactions between the functional domains and the domain to which the target system belongs.
This approach supposes that the need has been expressed clearly in functional terms.
The purpose of this activity is to formalise the conceptual architecture of the information system (IS), in order to establish the boundaries of the target system and characterise it. Sometimes it is possible to obtain the studies used to establish the IS (conceptual communication and processing models based on [MERISE] for example).

Decomposition into functional domains provides an overall view of the operation of the IS and possible links with external actors. This division will make it easier to situate the target system in the IS and to understand the issues at stake.

Generally any information system can be divided into:

- operational functions or operational support functions;
- support functions;
- activity checking and monitoring functions.

Operational functions arise from the organisation's missions.
Support functions arise from management of the means required to carry out the operational functions.
Finally, checking and monitoring functions concern management.

Changes in an operational function may have important consequences for the other functions. On the other hand, a change to a support or check function generally has no direct impact on operational functions.

Activity 1.2 - Study of the target system

The information system (IS) contributes, in part, to the achievement of the organisation's strategic objectives. To be able to extract all the elements useful for drawing up the security needs of the target system, a clear understanding of the IS and its operation is required. This is achieved by identifying the target system in the organisation's IS.

Present the target system

An overview of target system must be produced, clearly indicating its boundaries, relations with other domains or external actors and its purpose in the global information system.

List the issues at stake

At this stage of reflection, the strategic objectives should be known (see information systems master plan, opportunity study, etc.), the functional needs identified and defined, and target system constraints linked to information and organisation recorded. It is now appropriate to analyse the issues at stake and the context in which the target system is positioned.

This analysis identifies the strategic weight of the target system for the organisation and evaluates the level of importance of the functions in the target system. It consists in highlighting the impact of creating or operating the system, users' expectations, managers' expectations, the expected gains, etc. The issues at stake may be of a technical, financial or strategic nature.

List the essential elements

To describe the target system more accurately, the next operation consists in identifying the essential elements. This selection is carried out by a mixed work group representative of the IS (managers, computer specialists and users).

The essential elements are usually the core functions and information of the target system activity. Other essential elements such as the organisation's processes can also be considered. This second approach will be more appropriate for drawing up an information systems security policy, information systems security master plan or continuity plan. The essential elements are the information assets or "intangible assets" that need to be protected. Depending on the purpose, some studies will not require an exhaustive analysis of all the elements making up the target system. In such cases, the study boundaries can be limited to the vital elements of the target system.

The selection of essential elements is made with a manager who is or will be a user of the existing or future system. After an initial analysis, he indicates which elements are sensitive. The essential elements are usually functions or information for which the owner's or holder's responsibility would be called into question, or which would result in damage to the organisation or third parties, if their availability, integrity, confidentiality or other security criteria were not guaranteed.

The essential functions (or subfunctions) are mainly:

- functions whose loss or degradation make it impossible to carry out the mission of the system;
- functions that contain secret processing or processes involving high-level technology;
- functions that, if modified, can greatly affect the accomplishment of the system's mission.

The following cases may be the basis for identifying the sensitivity of information:

- information covered by defence secrecy defined in [IGI 900], for which the security requirement level cannot be negotiated;
- sensitive non-classified defence information as defined in [Rec 901] for which the requirement level can be negotiated in relation to the organisation's own environment considerations.

More generally, essential information mainly comprises:

- classified information that may or may not be covered by defence secrecy;
- vital information for the exercise of the organisation's mission or business;
- personal information, especially nominative information in the sense of the French law on information technology and civil liberties;
- 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.

Functions and information that are not identified as sensitive after this activity will have no defined security need (sensitivity) in the remainder of the study. This means that even if such functions or information are compromised, the system will still accomplish the mission successfully.
However, they will often inherit measures taken to protect the functions and information identified as sensitive.

The security needs (sensitivities) expression sheets will allow users to express their assessment of the sensitivity of the essential functions and information.

Produce a functional description of the target system

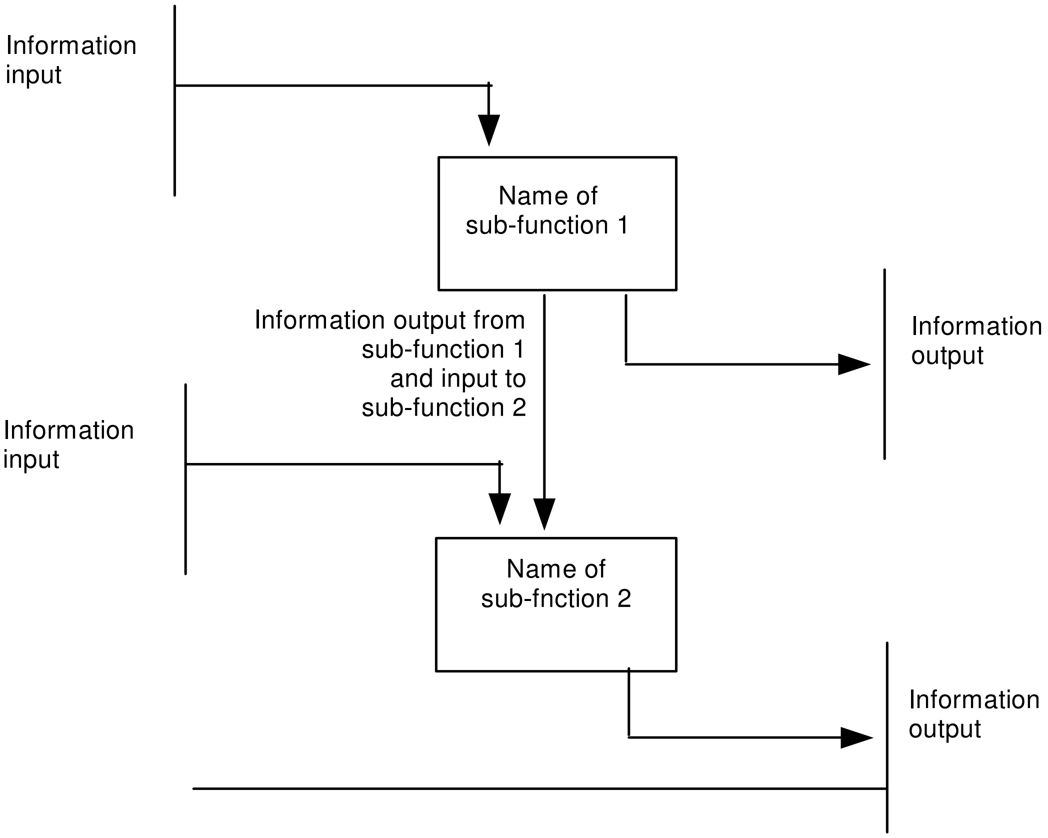
At this level, the objectives of the target system are clearly expressed and it is positioned in relation to the existing system. For each essential function identified this will require a precise indication of:

- the information input and output (required results);
- the processing required (also indicating the interfaces used by the target system to exchange information with the other information systems).

A function may be broken down into subfunctions, which are coherent sets of processing (aggregate of basic tasks) and information.

For a system still to be designed, the target system is modelled using the general design method selected (e.g. MERISE, SADT, UML, etc).

For an existing system, or if there was no modelling during its design, the following representation can be used: the functions are represented by a diagram using a top-down approach, showing the relationship between the subfunctions and the input and output information of the functions (see the example on the next page).



example : Representation of a human resources management function

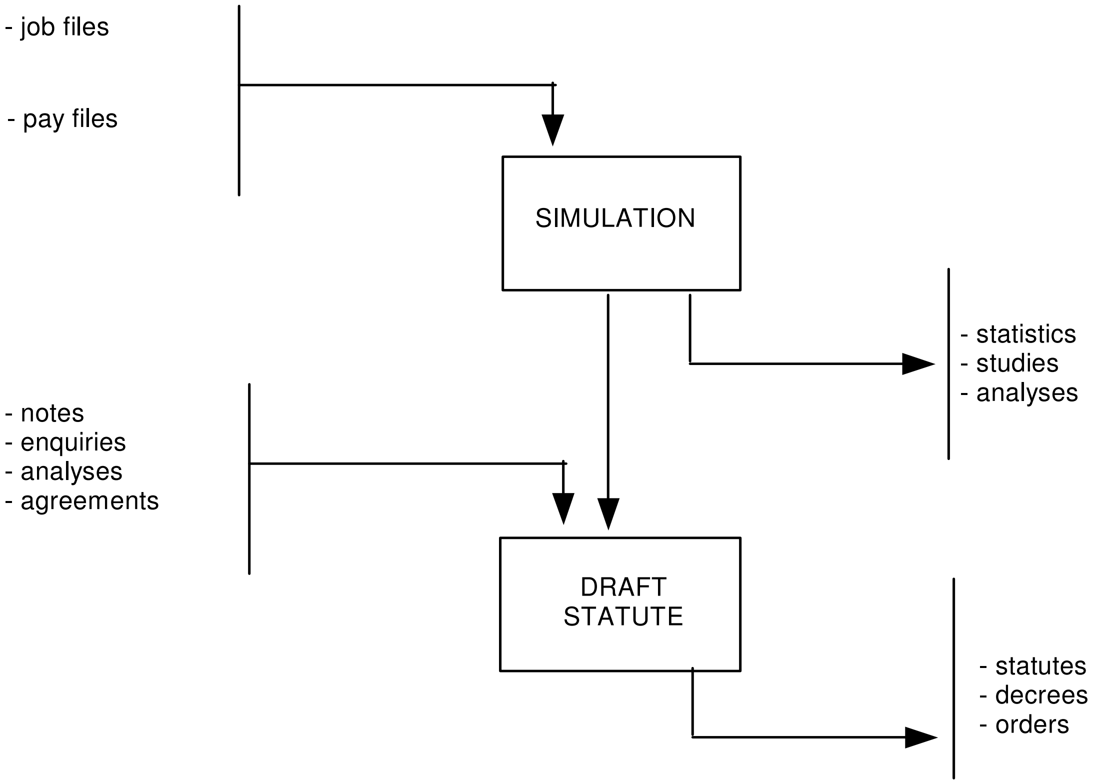


Figure 1 – Representation of the functions and information

Decomposition of the system into subsystems

The decomposition of the system into subsystems should be considered if it assists the remainder of the study.

The main objective of a decomposition into subsystems is to simplify the application of the EBIOS method. The study manager may therefore choose to break down the system into several subsystems. This will allow him to determine either several target systems more easily studied separately, or a single target system providing a clearly delineated subject of study.

Decomposition into subsystems is at the study manager's discretion. It is usually easier to study several subsystems than a global multiform system, but the number of subsystems must remain low (fewer than five) as each will be studied separately.

Decomposition into subsystems assists:

- ❑ in selecting where to concentrate the effort: it highlights subsystems where a study is pointless or of lower priority;
- ❑ in organising the study: a subsystem can be studied by a smaller team.

There is no strict method for breaking down a system into subsystems, but rather, a set of criteria to be examined. The main applicable decomposition criteria are as follows:

- ❑ Criterion 1: The hardware architecture

  Create as many subsystems as there are stand-alone machines (or sets of machines). If, in general, the machines are interconnected, decomposition depends on the level of interoperability of the various parts (machines or sets of machines) of the system.
  Example: increasing level of interoperability

  - Physically separated machines. Transfers by tapes or floppy disks.
  - Machines connected by a dedicated file transfer link.
  - Set of stand-alone machines co-operating via a local network.
  - Set of machines connected by a local network, equipped with the same operating system and administered centrally.

- ❑ Criterion 2: Functions or essential information

  It may be possible to decompose a physical subsystem on the basis of the functions provided by a given machine or part of the system or according to the way the most sensitive information is processed.

- ❑ Criterion 3: Single responsibility

  A set of entities forming a whole because there is a single responsibility for implementation (user group or technical implementation) can be taken as a subsystem to be studied separately. This may concern a part of a system placed under the responsibility of a department duly identified on the organisation chart. This criterion may also be applied if there are several separate documentation systems.

- ❑ Criterion 4: Distinct sub-zones

  If the components (equipment, media, personnel) are set up in different zones (building, reserved sub-zones, basements, etc.), each sub-zone could be considered as a subsystem provided that the level of interoperability with the outside is sufficiently low.

- ❑ Criterion 5: Isolation of "common subsystems"

  After applying the first four criteria, some sets of entities or components may be positioned at the intersection of several subsystems (common servers, common networks, common personnel or sub-zones for example). It may be possible to form these into subsystems to be studied separately. The results of these studies are then transferred to the enveloping subsystems. The process is roughly equivalent to work factorisation.

List the assumptions

The assumptions concerning the target system need to be formalised. Assumptions are usually imposed by the organisation in charge of the study, for reasons concerning the organisation's internal or external policy, or financial and planning reasons.
They may also constitute a risk accepted a priori for a given environment.
When writing a protection profile or security target, which must demonstrate that the security objectives fully cover the threats, they may be vulnerabilities that cannot be covered by a security objective during the following stages. In the same context, some assumptions may be the formalised acknowledgement of identified constraints, while others are only guides to understanding the context.

The following labelling system is proposed for assumptions: H.xx (H represents "assumption" ("hypothèse" in French) and xx the name of the assumption).

The special case of choosing the security operating mode.

Determining the security operating mode of the system consists in indicating how the system enables various categories of users to process, send or store information of varying sensitivity. It allows the general security issues to be understood since the security operating mode defines the information management context of an information system.

The security operating mode of the system usually belongs to one of the following categories:

- Category 1: exclusive operating mode
    - Everyone accessing the system is authorised for the highest classification level and has an identical need to know (or equivalent) with regard to all the information processed, stored or sent by the system.
- Category 2: dominant operating mode
    - Everyone accessing the system is authorised for the highest classification level but they do not have an identical need to know (or equivalent) with regard to the information processed, stored or sent by the system.
- Category 3: multilevel operating mode
    - Not everyone accessing the system is authorised for the highest classification level and they do not all have an identical need to know (or equivalent) with regard to the information processed, stored or sent by the system.

To choose the security operating mode of the system, it is important to know if the following exist or should exist:

- a prioritised information classification structure (e.g. confidential, secret, etc.) and/or compartmentalised structure (medical, company, nuclear, etc.),
- user categories,
- a notion of need to know, need to modify, need to have use of, etc.

The choice of security operating mode can be reassessed once the risks have been identified during the next stages. However, it is important to consider this aspect as early as possible, as its implementation has major consequences on IS and ISS architecture.

List the security rules

A study baseline and documents may have already been produced for information systems security; although a detailed analysis is not useful at this stage, information such as priorities, results, instructions, etc. can be looked for.
The aim is to identify the main rules and security measures, whether or not they are formalised. The following documents can be used for this:

- □ the information systems security policy;
- □ continuity plans for the applications;
- □ security instructions for developments;
- □ security audit results;
- □ security projects, etc.

The following labelling system is proposed for security rules: P.xx (P for policy and xx for the name of the security rule).

List the constraints affecting the target system

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

Constraints arising from pre-existing systems

Application projects are not necessarily developed simultaneously. Some depend on pre-existing systems. Even though a system can be broken down into subsystems it is not necessarily influenced by all the subsystems (and by extension, system functions) of another system.

Technical constraints

Technical constraints, of a physical nature, generally arise from installed hardware and software, and rooms or sites housing the IS:

- □ files (requirements concerning organisation, 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 setting up of security measures is often restricted by the budget that the organisation can commit. However, the financial constraint should still to be the last to take into account as the budget allocation for security can be negotiated on the basis of the security study.

Environment constraints

Environment constraints arise from the geographical or economic environment in which the IS is installed: country, climate, natural risks, geographical situation, economic climate, etc.

Time constraints

The time required for setting up security measures must be considered in relation to the upgradability of the IS; if the implementation time is very long, the risks for which the countermeasure was designed will have changed. Time is a determining factor for selecting solutions and priorities.

Constraints related to methods

Methods appropriate to the organisation's know-how will need to be imposed for aspects such as project planning, specifications, development and so on.
A set of organisational assumptions will be deduced and recorded on the basis of the information obtained.

Organisational constraints

Some lines for thought:

- ❑ operation (requirements concerning lead-times, supply of results, 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, organisation to be set up, etc.)
- ❑ management of external relations (requirements concerning organisation of third-party relations, contracts, etc.).

List the regulatory references specific to the target system.

Application of laws, rules or regulations may restrict the choice of physical solutions or procedures and modify the environment or work habits.

All regulatory measures applicable to the target system must therefore be identified.

Activity 1.3 - Determination of the security study target

List and describe the entities of the system

The target system consists of a set of technical and non-technical entities that must be identified and described. These entities have vulnerabilities that are exploitable by attack methods aiming to impair the intangible essential elements of the target system (functions and information). These are the entities that must be protected. They are of various types.

The entity types are presented in the following paragraphs (you are advised to use the entity types and subtypes from the guide "Tools for assessing ISS risks" to list and describe the system entities).

<u>Hardware</u>

Hardware includes all the physical elements of the information system, including active data processing media or passive data media.

<u>Software</u>

The software type consists of all the programmes contributing to the operation of a data processing set.

<u>Networks</u>

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

<u>Personnel</u>

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

<u>Sites</u>

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

<u>Organisations</u>

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

<u>Systems (optional)</u>

The system type consists of all specific facilities linked to information technologies, with a specific objective and an operational environment. It is composed of various entities belonging to other types described above. This type is useful when a macroscopic analysis is conducted.

For a better understanding of this type of entity, take the example of a network of on-board computers used to query vehicle data bases for surveillance operations.

Hardware types:

- ❑ *on-board terminal for land vehicles, of the type PC compatible laptop microcomputer querying a mini-data base;*
- ❑ *central server system with communications front-end and modular architecture querying a national data base.*

Software types:

- *central server operating system: high transactional processing capacity;*
- *relational data base management system operating in a two-level co-operative mode installed on the national server.*

Network types:

- *national X25 packet switched network (existing constraint);*
- *national-coverage radio network between the on-board terminals and the X25 national network.*

Personnel types:

- *application maintenance and development personnel: internal and external support;*
- *authorised and specialised information processing centre personnel using a technical platform;*
- *users of the on-board terminals: authorised personnel.*

Site types:

- *information processing centre protected by perimeter fence and video surveillance system in a geographical area not classified as a major risk site;*
- *light vehicles spread over the national territory.*

Organisation types:

- *development and leased maintenance support;*
- *local and central base updating procedures carried out by fixed-shift specialised teams directly connected to the national network.*

The entity types can be broken down into entity subtypes with a more detailed description.

Establish the link between essential elements and entities

This task highlights:

- the links between the essential functions and the entities contributing to the performance of these functions for the target system,
- the links between the essential information and the entities contributing to the processing of this information for the target system.

These links will be used when comparing threats and needs. They are represented by a matrix showing the essential elements and selected entities. The link between essential element and entity is shown in the table by one or more crosses where the essential element line intersects with the entities concerned by this essential element.

Example of an Essential elements / entities grid:

Entities	***HARDWARE***				***SOFTWARE***				***NETWORKS***				***PERSONNEL***					***SITES***			***ORGA.***		
Essential elements	***M1***	***M2***	***M3***	***M4***	***L1***	***L2***	***L3***	***L4***	***R1***	***R2***	***R3***	***R4***	***P1***	***P2***	***P3***	***P4***	***P5***	***S1***	***S2***	***S4***	***O1***	***O2***	***O3***
Function 1	+					+	+	+					+	+	+	+			+			+	+
…	+					+	+	+					+	+	+	+	+	+	+		+		+
Function N	+	+			+	+		+	+			+		+	+	+	+	+	+			+	+
Information 1	+		+		+	+		+		+		+		+	+	+	+	+	+			+	+
…	+			+	+	+		+			+	+		+	+	+	+	+	+			+	+
…	+					+	+	+					+	+	+	+			+	+	+	+	+
Information N	+					+	+	+					+	+	+	+	+	+	+	+			+

Step 2 - Expression of security needs

Activity 2.1 - Creation of needs sheets

Choose the security criteria to be taken into account.

The security needs associated with the functions and information are expressed according to the security criteria [2].. Three security criteria are essential:

- ❑ Availability (D): a property of essential elements allowing them to be accessed by authorised users at the required time.
  - o For a function: guaranteed continuity of processing services; absence of problems linked to response times in the wide sense.
  - o For information: a guarantee of the proposed availability for access to data (time-to-access and availability timetable); there is no total loss of information; so long as there is a back-up of the information, it is considered to be available. It is assumed that there is a back-up, and availability is assessed in terms of the back-up function for this information.
- ❑ Integrity (I): property defining the accuracy and completeness of the essential elements.
  - o For a function: assurance that the algorithm is correct or that automated or non-automated processing is implemented according to the specifications; no incorrect or incomplete results from the function.
  - o For information: guarantee that no operating errors or unauthorised uses have impaired the accuracy and exhaustiveness of the data; no corruption of the information.
- ❑ Confidentiality (C): property of essential elements making them only accessible to authorised users.
  - o For a function: protection of algorithms describing the management rules and results whose disclosure to unauthorised third parties could be harmful; non-disclosure of processing or a mechanism of a confidential nature.
  - o For information: protection of data whose disclosure to unauthorised third parties could be harmful; non-disclosure of data of a confidential nature

The needs can also be expressed in terms of Proof (accountability), Checking (auditability) and Anonymity or any other security criterion which, if breached for a function or information item, may jeopardise the potential benefits of the system:

- ❑ proof, checking: guarantee that the transmission or reception of information cannot be denied, with the possibility of auditing the results provided (e.g.: transfer of funds and verification of the ledger using the input information).
- ❑ anonymity: a measure that makes it impossible to identify anyone creating an information item (a voter for example) and/or carrying out an action (a telephone call for example) that is processed on the information system .
- ❑ reliability: consistency between expected behaviour and a result.
- ❑ …

Determine the scale of needs

The security needs must be expressed for each selected security criterion. Security needs must be graded in the form of levels of needs. To do so, each level of needs must be defined for each security criterion.

The scale usually has levels between 0 (no breach) and 4 (very serious breach). However, a scale with a different number of levels can be defined,

preferably keeping the same number of levels for all the security criteria.

As far as possible, the reference values must be explicit and include a set of limited values.

[2] Partly according to the "white book" on information system security in credit companies

This work is usually conducted using a table with the security criteria in the columns and the levels in the rows. The definitions appear where the rows and columns intersect.

The table below shows an example of a scale for the security criteria "availability, "integrity" and "confidentiality" with 5 levels.

Security needs	***Availability***	***Integrity***	***Confidentiality***
0	*No availability need*	*No integrity need*	*Public*
1	*Long term (specify)*	*[value not used]*	*Restricted*
2	*Medium term (specify)*	*Medium integrity need*	*Confidential (partners)*
3	*Short term (specify)*	*[value not used]*	*Confidential (internal)*
4	*Very short term (specify)*	*Total integrity*	*Secret*

This scale must be adapted to the study context with the assistance of the persons who will determine the needs. Each value will therefore be genuinely meaningful for them and the values will be consistent.

Determine the relevant impacts

The consequences of any damage can be assessed from several points of view. The significant impacts for the organisation must be identified by the manager using the system. They will indicate the domains prone to impact that should be considered and will provide elements justifying the security needs.

These impacts may be chosen from among those proposed below; however, this is not an exhaustive list and it must be adapted to the context studied:

- ❑ Interruption of service:
  - o inability to provide the service;
- ❑ Loss of customer confidence:
  - o loss of credibility in the internal information system;
  - o damage to reputation;
- ❑ Disruption of internal operation:
  - o disturbance for the organisation itself,
  - o additional internal costs;
- ❑ Disruption of a third party's operation:
  - o disturbance for third parties transacting with the organisation,
  - o various types of injury;
- ❑ Infringement of laws / regulations:
  - o impossibility of fulfilling legal obligations;
- ❑ Breach of contract:
  - o impossibility of fulfilling contractual obligations;
- ❑ Danger to personnel / user safety:
  - o danger for the organisation's personnel and / or users;
- ❑ Attack on users' private life;
- ❑ Financial losses;
- ❑ Financial costs for emergency or repair:
  - o in terms of personnel,
  - o in terms of equipment,
  - o in terms of studies, experts' reports;
- ❑ Loss of goods / funds / assets;
- ❑ Loss of clientele, 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;
- Etc.

These impacts are proposed as a guide. The work group must propose those that are most significant for the organisation and adapt them closely to it. The results of the previous activities, especially those linked to the study of the organisation, issues at stake and context of the system can be used to choose these impacts. The jeopardising of the organisation's missions, business or values must be taken as significant impacts. To make the impacts more objective, explicit examples of conceivable consequences must be provided for each one.

Once the security criteria and impacts are determined, needs expression sheets can be produced for each essential element.

Security needs expression sheet:

Name of the essential element	***Impact 1***	***…***	***Impact n***	***Security needs***	***Comments***
Security criterion 1	*B11*	*…*	*B1n*	*f(B11…B1n)*	
…	*…*	*…*	*…*	*…*	
Security criterion n	*Bn1*	*…*	*Bnn*	*f(Bn1…Bnn)*	

The security need summary for each essential element and each security criterion ("Security needs" column) will be determined on the basis of all the values expressed for each impact.

Additional damage items can be added to these sheets for each security criterion. This will assist the expression of security needs by considering various points of view.

Here are some examples of damage relating to the main security criteria (the situation and context should lead to listing specific damage for each criterion selected):

- for availability:
  - degrading of performance,
  - short interruption,
  - long interruption,
  - inaccessibility,
  - total loss (destruction);
- for integrity:
  - accidental modification,
  - deliberate modification,
  - incorrect results,
  - incomplete results;
- for confidentiality:
  - internal disclosure,
  - external disclosure.

Security needs expression sheet with additional items:

Name of the sensitive element	***Damage***	***Impact 1***	***…***	***Impact n***	***Security needs***	***Comments***
Security criterion 1	*Damage 1*	*B111*	*…*	*B11n*	*f(B111…B1nn)*	
Security criterion 1	*…*	*…*	*…*	*…*		
Security criterion 1	*Damage n*	*B1n1*	*…*	*B1nn*		
…	*…*	*…*	*…*	*…*	*…*	
Security criterion n	*Damage 1*	*Bn11*	*…*	*Bn1n*	*f(Bn11…Bnnn)*	
Security criterion n	*…*	*...*	*…*	*...*		
Security criterion n	*Damage n*	*Bnn1*	*…*	*Bnnn*		

In this case, the security need summary for each essential element and each security criterion ("Security needs" column) will be determined on the basis of all the values expressed for each impact and each kind of damage.

Activity 2.2 – Summary of security needs

Assign a security need per security criterion to each essential element

For a successful study, a mixed work group representative of the IS (managers, computer specialists and users) must be set up. This group will discuss the security needs expressed and the justifications.

Collection of security needs

Security needs are collected using the security needs expression sheets and the scale of needs given to the users concerned. The values filled in reflect the point of view of the users with regard to their security need. This point of view can be justified by a comment (especially for extreme values). A summary of the sheet must be produced in order to obtain a vector of security needs for each essential element.

The users themselves must produce this evaluation by expressing the acceptable values which must not be exceeded. They assign a rating at each row-column intersection of the needs expression sheets to obtain a vector of availability - integrity- confidentiality. However, the system users are not necessarily experts in IS security, nor trained in ISS awareness. The work group or persons carrying out the interviews with this population therefore have an important role to play in ensuring that the scale of needs is well understood and that the results obtained are consistent.

The security needs are independent of the risks incurred and the security means set up. They therefore represent an intrinsic value of the sensitivity of information, functions or sub-functions. For example, in the field of defence, assigning a confidentiality value to documents is equivalent to classifying them (secret-defence, confidential-defence, etc.).

If an essential element has needs that vary over time, the various statuses must each be studied as separate essential elements.

All the security needs expression sheets should be completed to obtain risks with accurately formulated impacts.

Summary of security needs

The work group fills in the results obtained from users on the security needs summary sheet and determines the value taken as the summary value. This summary value, a consensus of the various points of views, is then validated. The person who validates it must have a global view of the essential elements (for example the manager using the system, or the owner of the essential elements). A consensus can be obtained by each contributor expressing his/her rationale followed by arbitration. In the last resort, the security needs summary value based on the security criteria of an essential element can be taken as the maximum value assigned by the users on each of the sheets.

If divergence is too great, it may be necessary to ask users to reconsider their values or provide a fuller explanation. The summary must, in every case, be justified in relation to the organisation's important elements highlighted during the context study.

Example of a security needs summary sheet:

List of essential elements	***Summary of security needs***		
	Confidentiality	***Integrity***	***Availability***
Function 1	*0*	*3*	*3*
Function 2	*1*	*3*	*2*
…	*…*	*…*	*…*
Function n	*0*	*4*	*2*
Information 1	*2*	*1*	*1*
…	*…*	*…*	*…*
Information n	*4*	*3*	*0*

Step 3 - Threat study

Activity 3.1 - Study of threat sources

List the relevant attack methods

Selection of attack methods should be based on the list of generic attack methods and threat agents proposed in the guide "Tools for assessing ISS risks". The attack methods considered to be relevant to the context, missions and entities making up the target system should be retained. The selection is made with the work group using a theme-based list of attack methods. The themes are:

- ❑ physical damage
- ❑ natural event
- ❑ loss of essential services
- ❑ disturbance due to radiation
- ❑ compromise of information
- ❑ technical failures
- ❑ unauthorised actions
- ❑ compromise of functions

This classification allows easier selection of the relevant attack methods. Some themes (physical damage, natural events, loss of essential services) can be dismissed if justification can be provided. For example, the subject may have been covered by previous studies.

An attack method must be retained if it is realistically achievable and if it has a probable impact.

It is advisable to explain why an attack method or theme has not been selected so that the choices made can be traced. To make traceability of the choices as clear as possible, all the non-selected attack methods can be transformed into assumptions (remembering that several non-selected attack methods can be grouped as a single assumption).

The attack methods proposed in the knowledge bases are said to be "generic" because they define a category which may contain attack methods described with a much finer degree of granularity. The proposed list can therefore claim to be exhaustive in so far as it remains possible to enter a specific attack method in a proposed category. However, this list can be adapted to the context of the organisation and its use of the target system.

Attack methods can also be obtained from security studies conducted on similar systems or taken from documents with a general scope (security policy, security charter).

Characterise the attack methods according to the security criteria they may affect

Each attack method may affect at least one security criterion (availability, integrity, confidentiality, etc.).
All the retained attack methods should therefore by characterised according to the security criteria they may breach. This characterisation consists in determining the direct impacts on the security criteria, rather than all the possibilities implied.
Example: Fire affects primarily the availability criterion, although it may also affect integrity and confidentiality as a consequence; fire is therefore usually characterised by a breach of availability.
Characterisation of each attack method by security criteria (identical to those used for expressing security needs) makes it much easier at the next step to compare the security needs with the threats in order to determine the real risks.

Characterise the associated threat agents according to their type and causes

The attack methods are used by threat agents which must be characterised for each attack method. Their description must include:

- the type of threat agent (natural, human or environmental, i.e. outside the target system),
- the causes of each threat agent (accidental or deliberate); they may be refined by indicating the exposure level and available resources in the event of an accidental cause and specifying the expertise, available resources and motivation for a deliberate cause.

To characterise threat agents, you are recommended to use the section of the guide "Tools for assessing ISS risks" dealing with generic attack methods and threat agents.

The threat typology proposed in [IGI 900] and [Rec 901] can also be applied. This allows causes such as amusement, greed, strategic gain or terrorism to be specified.

Add a value representing the attack potential of the threat agent

Characterisation of threat agents can be summarised by a single value for each attack method selected. This value is the attack potential, usually represented by one of the following values:

- 1 (accidental and random),
- 2 (limited opportunities or resources),
- 3 (high level of expertise, opportunity and resources).

This attack potential can be used to determine an adequate strength level for the security objectives.

The table below presents an example of selection and characterisation of attack methods:

		Threat elements						***Security criteria affected***		
		Type			***Cause***					
	Attack methods	***Natural***	***Human.***	***Environmental***	***Accidental***	***Deliberate***	***Attack potential***	***Availability***	***Integrity***	***Confidentiality***
1	*Fire*	*+*	*+*	*+*	*+*	*+*	*2*	*+*	*+*	
13	*Loss of means of telecommunication*			*+*	*+*	*+*	*1*	*+*		
19	*Eavesdropping*		*+*	*+*		*+*	*2*			*+*
20	*Theft of media or documents*			*+*		*+*	*2*			*+*
21	*Theft of equipment*			*+*		*+*	*1*	*+*		*+*
23	*Divulgation*		*+*	*+*	*+*	*+*	*1*			*+*
26	*Tampering with software*			*+*		*+*	*1*	*+*	*+*	*+*
42	*Attack on availability of personnel*	*+*	*+*	*+*	*+*	*+*	*1*	*+*		

Highlight the non-retained attack methods, with justifications

The dismissing of any attack method must be justified. Regardless of the reason - considered improbable or without consequences, dealt with elsewhere or deliberately dismissed - it is important to explain why it is not retained as it will not be studied during the remainder of the study even though it could be the source of risks for the organisation.

Activity 3.2 - Study of vulnerabilities

Identify the vulnerabilities of the entities according to attack methods.

For each attack method selected, the vulnerabilities of the target system making the attack possible must be determined. You are recommended to use the generic vulnerabilities from the guide "Tools for assessing ISS risks" to identify the vulnerabilities according to the type and sub-type of entity and the attack methods.

A vulnerability is a characteristic of the system that could be exploited by a threat agent to carry out an attack method. This characteristic, associated with the system entities, may constitute a security weakness or flaw.
Examples:

- ❑ *For a hardware type entity, the characteristics include the possibility of emitting radiation or the appeal of the equipment (laptop computer);*
- ❑ *For a site type entity, the characteristics include ease of entry.*

These characteristics become vulnerabilities if they can be exploited by attack methods:

- ❑ *The use of laptop computers is a vulnerability in terms of the "theft of equipment" attack method;*
- ❑ *The possibility of emitting radiation is a vulnerability in terms of the "interception of compromising stray signals" attack method.*

An attack method may exploit several vulnerabilities.
Example: The "tampering with hardware" attack method becomes achievable if:

- ❑ *it is easy to enter the site (vulnerability of the "site" entity);*
- ❑ *components can be added to the hardware (vulnerability of "hardware" and "software" entities)*
- ❑ *there is no equipment monitoring plan (vulnerability of "organisation" entity).*

A list of generic vulnerabilities associated with each attack method and each entity sub-type is provided in the knowledge bases). The selection is made from this list, but it may also be based on elements specific to the system. It is important to note that the proposed list is a basis of reflection that can be personalised and must be adapted to the context studied. This list is necessarily open to continual change.

Where appropriate, estimate the level of vulnerabilities

Vulnerabilities can be characterised by their level, representing the possibility of achieving the attack methods that exploit them.

This level is assessed according to several criteria:

- ❑ concerning the specific context of the system;
- ❑ concerning the state of the art in the area concerned.

In many cases, there are no statistical data allowing behavioural laws to be drawn up for the information system. The figures required for evaluation by quantitative techniques are only available for natural and technological risks, but it must be stressed that these analyses are subjective by their very nature.

The purpose of estimating the level of vulnerabilities is to ensure that only relevant vulnerabilities are retained and then prioritised. Simply selecting them may be sufficient, but the estimation of this value provides an additional level of detail.

The following scale can be used:

0	*Totally improbable or unfeasible*
1	*Low probability or needing very considerable means and/or a very high level of knowledge in the field concerned*
2	*Medium probability or needing some degree of expertise and/or specific equipment*
3	*High probability or possible using standard means and/or basic knowledge*
4	*Certain or possible for anyone*

For natural or human attack methods, the estimation of the vulnerability level is based on their observed feasibility. The level of vulnerability to abuse is estimated according to feasibility based on the equipment, competency and knowledge required.

This provides the list of estimated vulnerabilities associated with the selected attack methods for each type of sub-type of entity.

The following table shows an example of the result.

Attack methods		*Vulnerabilities*	*Hardware and software*	*Internal networks*	*External networks*	*Site*	*Personnel*	*Organisation*
1	*Fire*	*Fire prevention measures not consistent with the information system*				*2*		
		No instructions (warning, prevention, training, etc.)						*2*
		No organisation of fire safety						*3*
13	*Loss of means of telecommunication*	*Operating faults on the internal telephone network*				*1*		
		Malfunction of external networks (PSTN)			*1*			
		Malfunction of external networks (network services)			*1*			
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*

Activity 3.3 – Formalisation of threats

Formulate the threats explicitly

The formulation of threats may contain a varying amount of information. The essential point is to express an attack scenario explicitly, with the level of detail varying according to the purpose of the study.

In the best case, the threat formulation contains:

- ❑ The threat agent with its characteristics, especially its attack potential,
- ❑ The attack method used by the threat agent and the security criteria affected,
- ❑ The vulnerabilities exploited and their level,
- ❑ The entities presenting these vulnerabilities.

The threats can be characterised by an opportunity value determined according to the level of vulnerabilities exploited.
Although they are subjective, opportunity values have the advantage of being interrelated values.
If a threat involves the exploitation of a single vulnerability, the threat opportunity is equal to the level of the vulnerability.
If a threat involves the exploitation of several vulnerabilities, the threat opportunity has to be determined according to the respective levels of the vulnerabilities:

- ❑ generally by reconsidering the threat opportunity,
- ❑ either by retaining the lowest level of the vulnerabilities if the threat can only materialise by exploiting all the vulnerabilities,
- ❑ or by retaining the highest level of the vulnerabilities if the threat can materialise by exploiting just one of the vulnerabilities.

Example:

Threats		*Attack method*	*Attack potential*	*D*	*I*	*C*	*Opportunity*
M.INCENDIE	*Consequences of a fire aggravated because the fire prevention measures are inconsistent with the information system (site of the office), or there are no fire safety instructions or arrangements (organisation of the office)*	*1*	*2*	*+*			*2*
M.TELECOM	*Loss of means of telecommunication because of a malfunction of external networks (Internet)*	*12*	*1*	*+*			*1*
M.VOL-DOC	*Theft of media or documents by a visitor or cleaning personnel because the premises are easy to enter during working hours (site of the office)*	*19*	*2*			*+*	*3*
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*

Where appropriate, prioritise the threats according to their opportunity

The resulting list of threats can be sorted in decreasing order of threat opportunity. This list is a communication tool that should receive considerable attention. It provides the most explicit expression possible of what the organisation is exposed to. Threats with a high opportunity level should appear at the top of the list so that the persons concerned are fully aware.

Step 4 – Identification of security objectives

Activity 4.1 – Comparison of threats with needs

Determine the risks by comparing threats with securities needs

To determine the risks confronted by the organisation, the manner in which the essential elements can be affected by the threats must be highlighted, i.e. determine how the elements considered important by the organisation can be affected by what it is exposed to.

This link is created by comparing the threats with the needs. The security needs of the essential elements have been expressed according to various safety criteria (availability, integrity, confidentiality, etc.). The threats have been characterised in terms of the safety criteria that they can affect (on the basis of the characterisation of attack methods and according to the same security criteria). Now each essential element can be compared with each threat according to the security criteria in order to determine the possible consequences if the threats materialise.

A table listing the attack methods is produced for each essential element. The attack methods retained at this stage of the study are only those likely to exploit the vulnerabilities of the essential element. This is checked using the tables of entity / element links prepared during the context study. The security needs of the essential element studies and the security criteria that may be affected by each retained attack method are then transferred.

The sheets can be produced for each attack method or refined according to the threat, but the useful information is how the security criteria are affected by the attack methods. They are therefore transferred to each corresponding threat. It is possible to use the threats as factors instead of the attack methods, but it is the breaches caused by the attack methods that are compared with the needs, which is why the attack methods are usually taken as the factors of this operation.

The following rules are therefore applied for each security criterion:

- ❑ if a security criterion cannot be affected, the security needs concerned are nil;
- ❑ if a security criterion can be affected, the security needs concerned are equal to the security needs of the element considered.

Example:

I.VISU (Display)		*Security needs.*			*D*	*I*	*C*
					2	*2*	*0*
Attack methods		*Breach*			***Security needs concerned***		
		D	*I*	*C*	***D***	***I***	***C***
1	*Fire*	*+*	*+*		*2*	*2*	
13	*Loss of means of telecommunication*	*+*			*2*		
19	*Eavesdropping*			*+*			
20	*Theft of media or documents*			*+*			
21	*Theft of equipment*	*+*		*+*	*2*		
23	*External disclosure*			*+*			
26	*Tampering with software*	*+*	*+*	*+*	*2*	*2*	
42	*Attack on availability of personnel*	*+*			*2*		
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*

The resulting values represent the risk for the organisation since they integrate the need value.

The aim is to determine the risks of breach of the security needs of the essential elements. If a threat materialises it is likely to breach these needs with repercussions on the major impacts identified used to establish the needs.

The set of tables can then be summarised to provide a global view of the risks. This summary can be conducted using the attack methods or threats. Using this summary, reflection is steered towards the real impact of the threats on the essential elements, and therefore on the organisation itself.

Example of risk summary based on attack methods:

Risk summary				*Element 1*			*…*			*Element N*		
				D	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
				3	*2*	*0*	*…*	*…*	*…*	*0*	*1*	*0*
				Security needs concerned								
Attack methods	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*	*D*	*I*	*C*
Eavesdropping			*X*	*0*	*0*	*0*	*…*	*…*	*…*	*0*	*0*	*0*
Theft of equipment	*X*		*X*	*3*	*0*	*0*	*…*	*…*	*…*	*0*	*0*	*0*
…	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*	*…*

This allows the maximum values of the security needs concerned by the threat or attack method to be determined. This will be used as an element in prioritising the risks.

Formulate the risks explicitly

Using the risk summary table, the formulation of threats and possibly the scale of needs, the title of the risks must be formulated as explicitly as possible. The level of detail of the formulation depends on the required granularity.

In the best case, the formulation of the threat includes:

- □ the threat agent with its characteristics, especially its attack potential,
- □ the attack method used by the threat agent,
- □ the vulnerabilities exploited,
- □ the entities presenting these vulnerabilities,
- □ the threat opportunity,
- □ the main security needs concerned,
- □ the impacts on the organisation (based on the scale of needs).

Example:

Risks		*Maximum of the security needs concerned*	*The threat opportunity*	*Attack potential*
R.PIEGEAGE	*An intruder tampers with the software by modifying the system commands, installing pirated programmes, modifying an application (hardware, software and Internet) or acting on the system resource software (via Internet), thereby breaching the confidentiality of sensitive information (estimates, contentious issues file, etc.) and the integrity of essential elements (calculate the structures, estimates, technical plan, technical parameters, litigation file, etc.)*	*4*	*3*	*1*
R.VOL-VISITEUR	*Because of easy access to the premises (site of the office), a visitor or cleaner steals equipment known to be especially tempting (trading/technological value of most of the equipment, software and network elements) thereby breaching the availability of several essential elements and the confidentiality of sensitive information (estimates, litigation file, etc.)*	*2*	*1*	*1*
…	*…*	*…*	*…*	*…*

Prioritise the risks according to the impact on the essential elements and the threat opportunity

The resulting list of risks can be sorted in decreasing order of the maximum values of the security needs concerned and in decreasing order of opportunity for the threats concerned. This list is a communication tool that should receive considerable attention. It provides the most explicit expression possible of the real risks affecting the organisation. The risks that could affect the greatest security needs and for which the threat opportunity is high should therefore appear at the top of the list so that the persons concerned are fully aware. They can then be treated as priorities.

Another means of prioritising the risks, and at the same time guarantee the involvement of the persons concerned, is to have these persons prioritise the risks. Since these are the ones who decide whether or not to consider and treat each risk it is important that they should be involved at this level of the study.

Another possibility is to prioritise the risks using the first method and have the priorities checked using the second method.

Highlight the non-retained risks, with justifications.

The work group can suggest ruling out risks that only slightly affect the security needs and for which the threat opportunity is low. These risks must therefore be highlighted with a clear justification of why they are ruled out as they constitute residual risks for the organisation.

Activity 4.2 – Formalisation of security objectives

List the security objectives

The security objectives must cover all the risks that it has been decided to cover, taking into account the assumptions, security rules and various context elements (especially the constraints and issues at stake). They must be consistent with the operational objective or declared "product" objective of the target system and any knowledge of its physical environment.

The security objectives usually consist of the expression of the contracting authority's will to cover the risks, without specifying the solutions for achieving this.
They will therefore constitute a complete specification, which remains open as to the solutions to adopt and is perfectly adapted to the issues facing the organisation.

The risk components that the security objectives may deal with are:

- ❑ the threat sources (attack methods and threat agents),
- ❑ the vulnerabilities exploited (it is possible to use the generic security objectives and table for determining security objectives and requirements from the guide "Tools for treating ISS risks" in order to list the security objectives covering the vulnerabilities,
- ❑ the consequences (essential elements affected and impacts on the organisation).

The following labelling system is proposed for security objectives: O.xx (O for technical Objective and xx for the name of the security objective).

Examples:

O.INC-ORIGINE	*Measures must be taken to avoid an outbreak of fire*
O.INC-CSQ	*Measures must be taken to reduce the effect of a fire on the essential elements and in terms of financial loss*
O.INC-COHERENCE	*The site of the office must have fire prevention measures consistent with the information system*
O.INC-ORGA	*The organisation of the office must include fire safety instructions and arrangements*
O.TELECOM-ORIGINE	*Measures must be taken to avoid malfunction of the external networks*
O.TELECOM-CSQ	*Measures must be taken to reduce the effect of external network malfunction on the essential elements and in terms of disruption of internal operation*
O.TELECOM	*External network malfunction must not disturb the use of Internet by the office users*

Justify the fullness of coverage

The purpose of the security objectives determined above is to counter or minimise the risks affecting the target system and to take account of the assumptions and security rules.
The persons conducting the study must now check that they are necessary and sufficient for covering all the identified risks, assumptions and security rules.

The initial stage of justification consists in demonstrating that the security objectives:

- ❑ adequately cover all the risks,
- ❑ cover the security rules (and regulatory references),
- ❑ are relevant given the assumptions and issues at stake for the target system.

It is important to check that each security objective is compatible with the constraints affecting the organisation and target systems.

Coverage can then be summarised by a value from the following scale:

0	No cover
1	Partial cover
2	Complete cover

Example:

Risks	*Security objectives*	*Justification of coverage*	*Coverage*	*Attack potential*
R.PIEGEAGE	*O.SYS-COMMANDES* *O.SYS-ACTIONS*	*Both security objectives cover all the vulnerabilities exploited in the risk:* - *possibility of modifying system commands via Internet,* - *possibility of installing pirated programmes via Internet* - *possibility of modifying application software via Internet,* - *possibility of acting on the system resource software via Internet.*	*2*	*1*
R.VOL-VISITEUR	*O.LOCAUX* *O.VOL-PROTECTION* *O.PRISE-EN-CHARGE* *O.AUTH-DOC*	*The first two security objectives cover the vulnerabilities exploited in the risk:* - *ease of access to the office,* - *equipment recognised as particularly tempting (trading and technological value)* *The third security objective assists in reducing the risk by increasing users' responsibility.* *The last security objective ensures that the document writer is authenticated.*	*2*	*1*
…	…	…	…	…

The second stage of justification consists in demonstrating that each security objective is a response to at least one risk, one security rule (or regulatory reference) or one assumption (or issue at stake for the target system or security operating mode).

Example:

Security objectives	*R.PIEGEAGE*	*R.VOL-VISITEUR*	*R.VOL-RIGUEUR*	*R.VOL-UTIL*	*R.VIRUS-VERIF*	*R.INCENDIE*	*R.VIRUS-MAIL*	*R.PABX*	*R.TELECOM*	*R.MALADIE*	*R.VOL-DOC*	*R.ECOUTE*	*R.PERTE-DOC*	*R.DIVULGATION*
O.INC-COHERENCE						+								
O.INC-ORGA						+								
O.TELECOM									+					
O.ECOUTE												+		
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Where appropriate, classify the security objectives into two categories

The purpose of determining security objectives is to treat all security concerns and to declare the security aspects, which are:

- ❑ either taken into account directly by the target system (these are the security objectives concerning the target system)
- ❑ or taken into account by its environment (these are the security objectives concerning the target system environment).

Determination is based on an analysis of the resulting impacts on development (technical credibility, calendar, etc.), the security policy (conformity with the general policy elements), economic factors (costs incurred by taking technical or organisation measures into account) and the decisions to accept risks (for which the threat opportunity is negligible or for which external measures, such as insurance policies, can be taken).

Highlight lack of coverage, with justifications

The work group may decide not to cover all the risks, security rules or assumptions by security objectives. This lack of coverage must be highlighted and duly justified as it introduces residual risks for the organisation.

Examples:

- ❑ *A personnel member working on a contract discloses information to a competitor because of the ease of information exchange via the office's hardware, software and networks, and thereby breaches the confidentiality of sensitive information (estimates, litigation files, etc.).*
- ❑ *A personnel member working on a contract discloses information to a competitor because of the lack of procedures for monitoring the use of communication tools, and thereby breaches the confidentiality of sensitive information (estimates, litigation files, etc.).*

Activity 4.3 – Determination of security levels

Determine the adequate level of strength for each security objective

The required strength[3] of security measures meeting the security objectives is determined essentially on the basis of the attack potential of the threat agents at the source of the risks affecting the organisation. The protection level therefore depends on the attacker's level.

However, it also depends on other factors, such as the security needs of essential elements that may be affected, the threat opportunity, the general context, etc.

We shall consider three strength levels, expressing the minimum effort assumed to be necessary in order to disrupt the required security behaviour by direct attack on the underlying security mechanisms:

1 - Basic level A level of strength that, as shown by the analysis, allows the function concerned to provide adequate protection against a random violation of system security by attackers with a low attack potential.

2 - Medium level A level of strength that, as shown by the analysis, allows the function concerned to provide adequate protection against easily-implemented or intentional violation of the security system by attackers with a moderate attack potential.

3 - High level A level of strength that, as shown by the analysis, allows the function concerned to provide adequate protection against deliberately planned or organised violation of the security system by attackers with a high attack potential.

The required strength of security objectives covering the risks depends on the attack potential. If a security objective covers several risks with different attack potentials, the highest level is taken. This value has to be adjusted by taking into account the security needs of essential elements that may be affected, the threat opportunity, the general context, etc.
The level required for security objectives covering the security rules (or regulatory references) is chosen by the organisation on the basis of the importance it attaches to these rules and the effort it plans to make to have them observed.

The strength of each security objective must be justified.

[3] Levels taken from the definition of strength of function levels in ISO/IEC 15408.

Choose the level of assurance requirements.

There are 7 predefined assurance levels [4] (known as EAL – *Evaluation Assurance Level*):

EAL 1	Functionally tested
EAL 2	Structurally tested
EAL 3	Methodically tested and checked
EAL 4	Methodically designed, tested and reviewed
EAL 5	Semi-formally designed and tested
EAL 6	Semi-formally verified design and tested
EAL 7	Formally verified design and tested

These levels are made up of increasingly rigorous components used to evaluate the implemented security.

The EAL represents the level of confidence that can be given to the implementation of the security objectives. More specifically, it concerns the implementation of security functional requirements, which are a refinement of the security objectives. The higher the EAL, the greater the organisation's guarantee concerning the security functional requirements. However, it is important to consider the cost of implementing assurance requirements, as well as the feasibility for the organisation or its suppliers.

There is no simple method for determining the assurance level, which remains primarily a financial or marketing choice.

If necessary, the EAL chosen can be augmented by other assurance components.

Furthermore, an organisation does not necessarily have to use the EAL notion. It can define its own assurance requirements, choosing them from existing components or even defining new components.

Security assurance requirements usually specify not only the desirable behaviour that should be present but also the undesirable behaviour that should be absent. It is normally possible to demonstrate, through use or testing, that desirable behaviour is present.
On the other hand, it is not always possible to demonstrate conclusively that non-desirable behaviour is absent. This is why tests and examination of design and implementation play an important role in reducing the risk of such behaviour being present. The elements of the rationale must therefore support the declaration that there is no undesirable behaviour.

[4] The assurance level represents a package of assurance components taken from Part 3 of ISO/IEC 15408 representing a level of the pre-defined assurance scale.

Step 5 – Determination of security requirements

Article 5.1 - Determination of the security functional requirements

List the security functional requirements

The security functional requirements represent the means of achieving the security objectives and therefore of treating the related ISS risks. They must be determined by, or with, the prime contractor (it is possible to use the generic security functional requirements and table for determining security objectives and requirements from the guide "Tools for treating ISS risks" in order to list the security functional requirements likely to satisfy the security objectives covering the identified vulnerabilities).

To reduce the ISS risks, the table below presents, as a guide only, the main types of security measure specified by the security functional requirements according to the risk components:

	Main risk components		
Main types of measure	Vulnerabilities	Threat sources (attack methods and threat agents).	Consequences (essential elements and impacts)
Prediction and preparation	X	X	X
Dissuasion		X	
Protection	X		
Detection	X	X	
Confinement		X	X
"Combating"	X		X
Retrieval			X
Restoration			X
Compensation			X

This table is a tool for determining security functional requirements. It ensures that the various possible types of measure are considered.

The security functional requirements contribute to the treatment of ISS risks, which may consist not only in reducing them, but also in rejecting, transferring or assuming them.
Rejection of a risk will result in security functional requirements for a structural modification of the target system situation that eliminates its exposure to the risk.
Transfer of a risk will result in specific security functional requirements such as signing insurance or service provider contracts.
If a risk is assumed, there will be no security functional requirement and it will be accepted that the security objectives are not fully satisfied. This will identify the residual risks.

The functional requirements are imposed on the target system functions specifically supporting information technology security and determining the required security behaviour and on the target system environment.
These functional requirements may be taken from ISO/IEC 15408 (Common Criteria) or created from scratch. It is strongly recommended that requirements only be created from scratch if it is shown that they deal with a functional aspect that does not exist in the components of ISO/IEC 15408.
The list of security functional requirements taken from the Common Criteria is made up of classes, families and functional components. There may be dependencies between the components. The dependencies appear when a component is not self-sufficient and depends on the presence of another component. There may be dependencies between functional components themselves and between functional and assurance components. Depending on how well the system is known, and the expertise of the work group, the components may be left unrefined on the understanding that they will be refined by the prime contractor.

ISO/IEC 15408 allows for the possibility of using functional requirements not contained in the list provided, in order to represent all the information technology security requirements. The following instructions must be applied if these extended functional requirements are incorporated:

- ❑ All the security functional requirements must be formulated with reference to functional requirement components. If none of the requirement components are easily applicable to all or some of the security requirements, the work group may formulate these requirements explicitly without reference to ISO/IEC 15408.
- ❑ For evaluation to be feasible, all extended functional requirements must be expressed clearly and unambiguously; the level of detail and manner of expressing the functional components existing in ISO/IEC 15408 must be used as models.
- ❑ The evaluation results obtained using the extended functional requirements must include a warning indicating how they were obtained.
- ❑ Extended functional requirements must be incorporated in compliance with the APE or ASE classes of Part 3 of ISO/IEC 15408, whenever appropriate.

In the best case, the formulation of a security functional requirement must be:

- ❑ S – specific (one actor, one domain at a time),
- ❑ M – measurable (with defined means of monitoring),
- ❑ A - attainable (possibly in several stages, providing the required resources),
- ❑ R - realistic (in terms of the actors and their ability),
- ❑ T - time-linked (with a deadline, lead-time, defined period).

To determine the security functional requirements, all the elements of the context must be taken into account, especially the budgetary and technical constraints.

Examples:

EF.INC-DETECT	*The premises of a firm of architects must be equipped with a fire detection system with remote alarm reporting to a supervision system which may be run by a service provider. These measures must be studied and set up by experts in the field. They must be tested at least once a year.*
EF.FOURN-ACCES	*An office must have at least two separate Internet access subscriptions.*
EF.MAINTENANCE	*A maintenance contract must guarantee the availability of internal and external communication means within a suitable lead-time given the issues at stake in the office's business (12 hours' unavailability).*
EF.CHIFFREMENT	*The confidentiality of electronic mail exchanges must be protected by a commercially available encryption system. The tools using the encryption keys must be covered by a management policy for these keys.*
EF.LOCAUX	*Outside persons entering the "business" part of the office must be accompanied.* *Maintenance or cleaning personnel or any other person outside the office must not enter the premises if the office members are absent.* *The premises must be protected by security locks whose keys are kept only by the Director and his deputy.*
…	*…*

Justify the adequacy of coverage of the security objectives

A coverage grid must be produced to check that all the security objectives concerning the target system or its environment are covered by at least one security functional requirement. Likewise, each security functional requirement must cover at least one of these security objectives.

The rationale of the security requirements must demonstrate that all security requirements are suitable for satisfying the security objectives and that they are linked to them. It must be possible to demonstrate:

- ❑ that the combination of individual functional requirement components satisfies the declared security objectives,
- ❑ that all the security requirements form an internally consistent whole, whose elements are mutually supporting,
- ❑ that the strength of the functions chosen, as well as any announced explicit function strength, is consistent with the security objectives.

The initial stage of justification therefore consists in demonstrating coverage of the security objectives.

Coverage can then be summarised by a value from the following scale:

0	No cover
1	Partial cover
2	Complete cover

Example:

Security objectives	*Resistance levels*	*Functional security requirements*	*Justification of coverage*	*Coverage*
O.INC-COHERENCE	*2*	*EF.INC-LUTTE*	*The consistency of the fire safety measures with the information system is taken into full consideration by the security requirement relating to fire fighting.*	*2*
O.PABX	*1*	*EF.MAINTENANCE* *EF.REPRISE*	***The disruption caused by an operating fault on the internal telephone network (PABX failure at the office site) is reduced by these security requirements but may still occur.***	***1***
O.TELECOM	*1*	*EF.FOURN-ACCES* *EF.MISES-A-JOUR* *EF.REPRISE*	*Malfunction of external networks is averted by the first security requirement. The other two reduce unavailability.*	*2*
O.ECOUTE	*2*	*EF.CHIFFREMENT*	*Encryption satisfies the confidentiality protection objective.* *The required strength can be achieved by writing a key management policy.*	*2*
…	*…*	*…*	*…*	*…*

The second stage of justification consists in demonstrating that each security functional requirement covers at least one security objective.

Example:

Security requirements	*O.INC-COHERENCE*	*O.INC-ORGA*	*O.PABX*	*O.TELECOM*	*O.ECOUTE*	*O.LOCAUX*	*O.PERS-SENSIB*	*O.VOL-PROTECTION*	*O.PRISE-EN-CHARGE*	*O.MANIPULATION*	*O.ORGA-SENSIB*	*O.MALICIEUX*	*O.SUPP-CONTRÔLE*	*O.SYS-COMMANDES*	*O.SYS-ACTIONS*	*O.MALADIE*	*O.PSSI*	*O.REGLEMENT*	*O.AUTH-DOC*
EF.INC-DETECT		+																	
EF.INC-LUTTE	+	+																	
EF.INC-CONSIGNES		+																	
EF.INC-ORGA		+																	
EF.MAINTENANCE			+																
EF.FOURN-ACCES				+															
EF.CHIFFREMENT					+														
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Highlight any lack of coverage, with justifications

A consensus must be reached concerning the means by which the security objectives are achieved. This consensus can only be obtained by comparing the risks incurred with the cost of security measures corresponding to the security functional requirements under consideration.
It is reasonable to consider the greatest and most likely risks first since the treatment of these risks may sometimes result in the treatment of other less important risks.

The work group may decide not to cover all the security objectives by security requirements. This lack of coverage must be highlighted and duly justified as it introduces residual risks for the organisation.

Examples:

- *Loss of telecommunication means through an operating fault on the internal telephone network (PABX failure at the office site); a continuity plan and guarantee of maintenance within 12 hours reduce the unavailability of these means.*
- *A personnel member, despite the awareness programme, succumbs to persuasion and discloses information to a competitor while working on a contract, thereby breaching the confidentiality of sensitive information (estimate, litigation file, etc.).*
- *An intruder tampers with the software by modifying the system commands via Internet, despite access restrictions on the connected machines, use of firewalls and regular software updating; this may breach confidentiality of sensitive information (estimate, litigation file, etc.) and the integrity of essential elements (calculate the structures, estimates, technical plan, technical parameters, litigation file, etc.)*

Classify the security functional requirements into two categories

The security requirements are the result of refining the security objectives into a set of:

- security requirements for the target system,
- security requirements for the environment.

If they are satisfied, they will guarantee that the security study target can satisfy its security objectives.

Where appropriate, justify the coverage of dependencies of security functional requirements

All dependencies between security requirements must be satisfied. For reasons of consistency, some security requirements imply the existence of other security requirements. The dependencies can be satisfied by including the functional component concerned in the security functional requirements of the target system or as a requirement for its environment.
There must be rigorous justification of failure to satisfy a dependency.

Article 5.2 – Determination of security assurance requirements

List the security assurance requirements

The security assurance requirements of ISO/IEC 15408 are imposed on the system developer's actions, the evidence elements produced and the evaluator's actions (for example, constraints concerning the rigour of the development process and requirements for identifying and analysing the impact of potential security vulnerabilities).

Assurance that the security objectives are achieved by the selected security functions arises from the two following factors:

- confidence in the conformity of implementation of the security functions, i.e. the estimation that they are implemented correctly,
- confidence in the effectiveness of the security functions, i.e. the estimation that they effectively satisfy the security objectives.

The security assurance requirements may be reformulated according to the purpose of the study so that their title is more accessible to the persons involved in the study.

Example of a raw title:

ACM_CAP.1 *Version numbers*

Objectives:

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Dependencies:

No dependencies.

Developer's tasks:

ACM_CAP.1.2D The developer shall provide a reference for the TOE.

Content and presentation of evidence elements:

ACM_CAP.1.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.1.2C The TOE shall be labelled with its reference.

Evaluator's tasks:

ACM_CAP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Example of reformulated title:

EA.NUM-VERSION *The office must have a unique reference (or equivalent, e.g. version number) of each version of the target system entities. This reference identifies them.*

Where appropriate, classify the security assurance requirements into two categories

The security assurance requirements can belong to one of the following categories:

- ❑ security assurance requirements concerning the target system,
- ❑ security assurance requirements concerning the target system environment.

Where appropriate, justify the coverage of dependencies of security assurance requirements

The security assurance requirements may depend on other requirements that should be taken into account to create a consistent set.
There must be a demonstration of the fullness of coverage.
There must be rigorous justification of failure to satisfy a dependency.

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