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 2
APPROACH

Version 2 – 05 February, 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tel 01 71 75 84 15 - Fax 01 71 75 84 00

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):

General Secretariat of National Defence
Central Information Systems Security Division (DCSSI)
Operations Subdivision
Advisory Office
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

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 Requirements 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 possible 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

Table of Illustrations

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 second section of the method. It presents the methodological approach in the form of descriptive sheets.

For each step there is a description, a diagram situating the step in the complete EBIOS approach and a flowchart describing the activities of the step.

Each activity is described under the following headings.

DESCRIPTION
Summary of the methodological approach and diagram showing the position of the activity in the step.

PREREQUISITE ACTIVITIES
Other activities that must be completed for the activity concerned.

INPUTS
Data required for implementation of the activity.

ACTIONS
Actions required to conduct the activity successfully.

OUTPUTS
Data produced by the actions of the activity.

PRACTICAL ADVICE
Comments and advice for implementation of the activity.

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

Presentation of the Approach

The method formalises an approach for assessing and treating risks in the field of information systems security.

It is applicable at the pre-design or to existing systems, over the entire scope of the information system or a smaller part of it.

It is broken down into five steps, shown in the following figure:

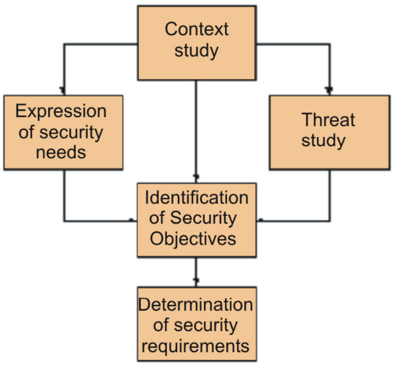
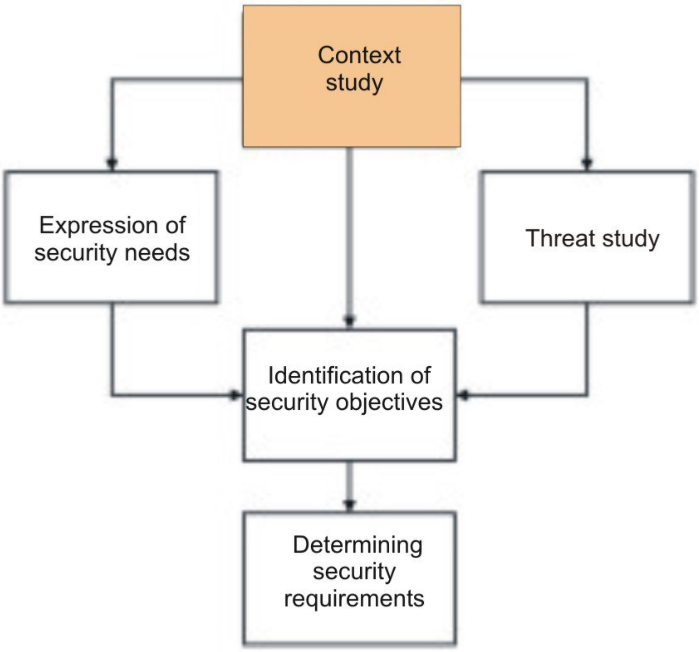

Context study
Expression of security needs
Threat study
Identification of Security Objectives
Determination of security requirements

Figure 1 – EBIOS global approach

- ❑ After the first step, the environment, purpose and operation of the target system are perfectly known and the essential element and entities on which they are based are identified.
- ❑ The second step contributes to risk assessment (risk estimation and definition of risk criteria). It allows the impacts to be formalised and the security needs of the essential elements to be evaluated in terms of availability, integrity and confidentiality, etc.
- ❑ The third step also forms part of risk assessment (risk analysis). It consists in identifying and describing the threats affecting the system. This is achieved by studying the attack methods and threat agents likely to use them, the exploitable vulnerabilities of the entities and the opportunities they present.
- ❑ The fourth step contributes to risk evaluation and treatment. During this step, the real risks affecting the system are formalised by comparing the threats (harmful events) with the security needs (consequences). They are covered by security objectives, consistent with the assumptions, security rules, regulatory references, operating mode and identified constraints which make up the security specifications.
- ❑ The fifth and last step belongs to risk treatment. It explains how to determine functional requirements allowing security objectives to be fulfilled and assurance requirements allowing the level of confidence in their fulfilment to be increased.

Step 1 - Context study


Context study
Expression of security needs
Threat study
Identification of security objectives
Determining security requirements

he purpose of this essential step is to identify the target system in global terms and position it in its environment so that the target of the security study can be accurately determined.

In particular, it allows the issues at stake for the system to be specified, together with the context in which it is used, the missions or services it must provide and the means used. It is also the stage at which all the information required for planning the study is collected.

After this step, the field of investigation for the study is clearly marked out, the assumptions, obligations and constraints are identified and the subjects to be dealt with are known.

The step is divided into three activities:

- ❑ Study of the organisation
- ❑ Study of the target system
- ❑ Determination of the security study target

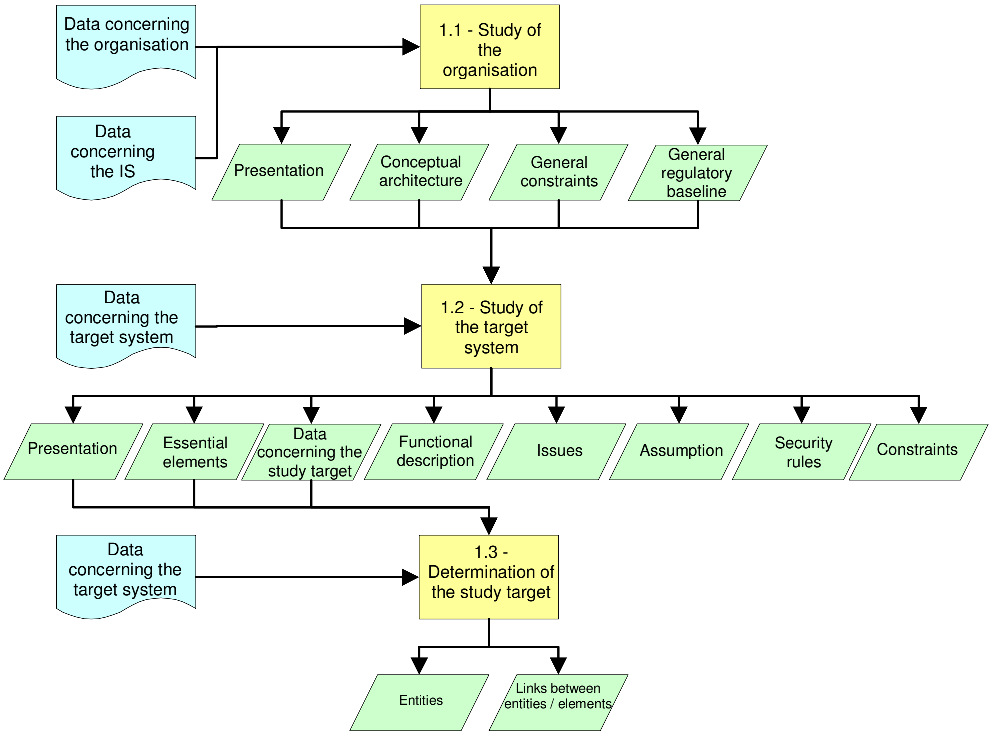
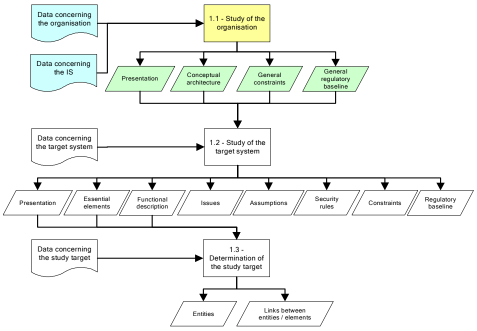

Data concerning the organisation
Data concerning the IS
1.1 - Study of the organisation
Presentation
Conceptual architecture
General constraints
General regulatory baseline
Data concerning the target system
1.2 - Study of the target system
Presentation
Essential elements
Data concerning the study target
Functional description
Issues
Assumption
Security rules
Constraints
Data concerning the target system
1.3 - Determination of the study target
Entities
Links between entities / elements

Figure 2 – Detailed flowchart of the study context

Activity 1.1 – Study of the organisation

DESCRIPTION

This activity consists in defining the study framework. General information about the organisation concerned by the security project must therefore be collected in order to gain a better understanding of its nature, organisation and the constraints affecting it. A global vision of the organisation's information system must also be obtained. During the ensuing activities these elements will be used to specify the issues at stake for this organisation's target system and to check that the security objectives and requirements are consistent with its missions.


Data concerning the organisation
Data concerning the IS
1.1 - Study of the organisation
Presentation
Conceptual architecture
General constraints
General regulatory baseline
Data concerning the target system
1.2 - Study of the target system
Presentation
Essential elements
Functional description
Issues
Assumptions
Security rules
Constraints
Regulatory baseline
Data concerning the study target
1.3 - Determination of the study target
Entities
Links between entities / elements

PREREQUISITE ACTIVITIES

None

INPUTS

- Data concerning the organisation and its information system (strategic documents, documents concerning the missions, powers and duties and organisation, documents concerning the information system, summaries of interviews with the organisation's managers).

ACTIONS

- Present the organisation
- List the constraints affecting the organisation.
- List the regulatory references applicable to the organisation.
- Produce a functional description of the global IS.

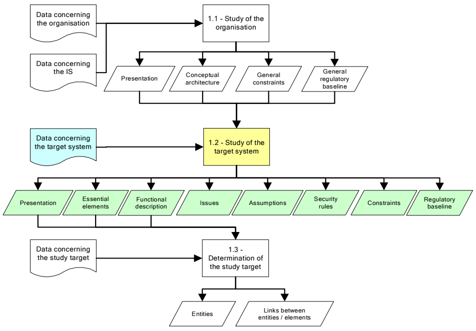
OUTPUTS

- Presentation of the organisation.
- List of general constraints affecting the organisation.
- List of general regulatory references applicable to the organisation.
- Conceptual architecture of the information system.

PRACTICAL ADVICE

- This first activity is essential for the rest of the study. It must provide the best possible understanding of the study context.
- A work group (or steering committee) must be set up, the persons to be met must be identified and interviews must be planned.
- An initial discussion must be held to check the nature of the problem originally posed and the competency of the team set up to handle it. This discussion must provide a maximum amount of information.
- The appropriateness of discussing a proposed subject must be assessed according to the scale of the project, the information collected before the discussion, the responsibilities of the interviewee, etc.
- The study of the organisation must involve its highest-level decision makers.
- Information is obtained from the operational managers involved in the study.
- Questionnaires are useful preparation for interviews and will provide a guide allowing the interviewees' responses to be easily formalised.

Activity 1.2 - Study of the target system


Data concerning the organisation
Data concerning the IS
1.1 - Study of the organisation
Presentation
Conceptual architecture
General constraints
General regulatory baseline
Data concerning the target system
1.2 - Study of the target system
Presentation
Essential elements
Functional description
Issues
Assumptions
Security rules
Constraints
Regulatory baseline
Data concerning the study target
1.3 - Determination of the study target
Entities
Links between entities / elements

DESCRIPTION

The purpose of this activity is to specify the context of use of the future or existing system. This requires specifying the subset of the organisation's information system constituting the target system and studying the issues at stake. The target system is then described and the assumptions, security rules and its constraints are identified.

PREREQUISITE ACTIVITIES

- ❑ Activity 1.1.

INPUTS

- ❑ Data concerning the target system.
- ❑ Presentation of the organisation.
- ❑ List of general constraints affecting the organisation.
- ❑ List of general regulatory references applicable to the organisation.
- ❑ Conceptual architecture of the information system.

ACTIONS

- ❑ Present the target system.
- ❑ List the issues at stake.
- ❑ List the essential elements.
- ❑ Produce a functional description of the target system.
- ❑ List the assumptions.
- ❑ List the security rules.
- ❑ List the constraints affecting the target system.
- ❑ List the regulatory references specific to the target system.

OUTPUTS

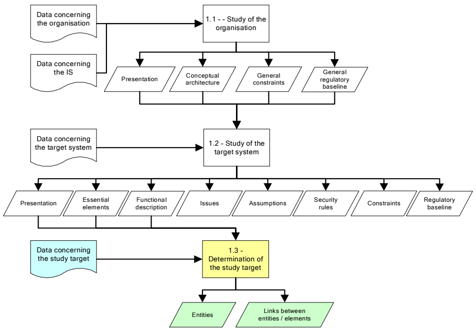
- ❑ Presentation of the target system.
- ❑ List of essential elements
- ❑ Functional description of the target system.
- ❑ List of issues at stake for the target system.
- ❑ List of assumptions.
- ❑ List of security rules.
- ❑ List of constraints specific to the target system.
- ❑ List of regulatory references specific to the target system.

PRACTICAL ADVICE

- ❑ The number and granularity of the essential elements will depend on the purpose of the study and nature of the target system. A study of a global information system aiming to provide an overview of the risks will not require the same detail as a study of a specific system for which formal approval is being sought.
- ❑ If system specifications are missing, the remainder of the security study may be called into question. There is little point in trying to protect a system that is not well known. On the other hand, it is possible to conduct a rapid, global study which must then be refined as more specifications become available.
- ❑ Division into subsystems can be considered for complex systems. In this case, several studies will have to be conducted in parallel.

Activity 1.3 - Determination of the security study target

DESCRIPTION


Data concerning the organisation
Data concerning the IS
1.1 - - Study of the organisation
Presentation
Conceptual architecture
General constraints
General regulatory baseline
Data concerning the target system
1.2 - Study of the target system
Presentation
Essential elements
Functional description
Issues
Assumptions
Security rules
Constraints
Regulatory baseline
Data concerning the study target
1.3 - Determination of the study target
Entities
Links between entities / elements

The purpose of this activity is to determine precisely the entities on which the essential elements (functions and information) of the target system rely. The activity consists in identifying and describing entities of all types: hardware, software, network, personnel, site or organisation. It also involves listing the essential elements that rely on each of these entities.

PREREQUISITE ACTIVITIES

- ❑ Activity 1.2.

INPUTS

- ❑ Data concerning the security study target.
- ❑ Presentation of the target system.
- ❑ List of essential elements
- ❑ Functional description of the target system.

ACTIONS

- ❑ List and describe the entities of the system.
- ❑ Establish the link between essential elements and entities.

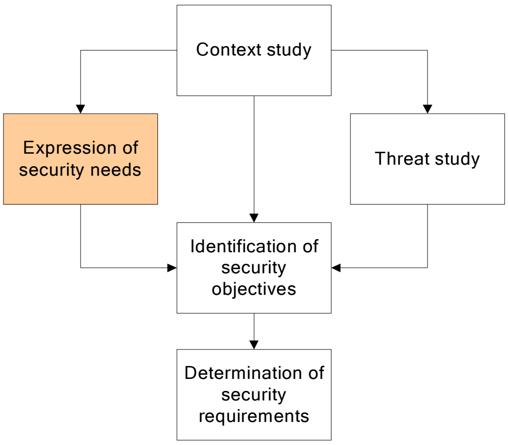
OUTPUTS

- ❑ List of entities.
- ❑ Entity / element tables.

PRACTICAL ADVICE

- ❑ It is advisable to use the entity types and subtypes from the guide "Tools for assessing ISS risks" to list and describe the system entities.
- ❑ It is important not to omit identifying the organisation entity (and likewise the site entity) for a target system based on a single type of organisation or site. For many target systems, certain types may be represented by just one entity. They must nevertheless be listed as they have vulnerabilities that must be taken into account in the study. Generally there will be at least one entity of each type.
- ❑ The entities on which the target system relies can also be added to the functional description by superimposing them on the diagrams. This provides a better view and understanding of the system.

Step 2 - Expression of security needs


Context study
Expression of security needs
Threat study
Identification of security objectives
Determination of security requirements

This step contributes to risk estimation and definition of risk criteria. It also allows system users to express their security needs for the functions and information they handle.

The expression of security needs results from the operational requirements of the system, independently of any technical solution.

It is based on the preparation and use of a scale of needs and the detection of impacts that are unacceptable for the organisation.

The expression of needs is also used to define the system operating mode, i.e. the general manner in which system users are managed.

The step is divided into two activities:

- ❑ Production of needs sheets.
- ❑ Summary of security needs

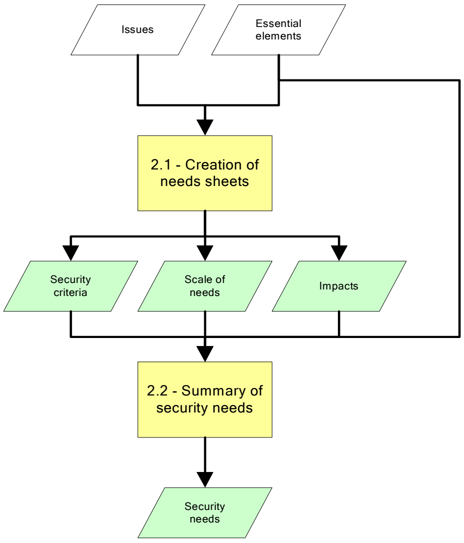
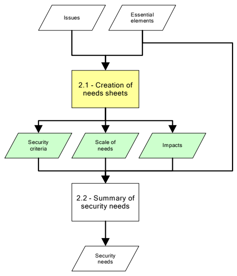


Figure 3 - Detailed flowchart of the expression of security needs

Activity 2.1 - Creation of needs sheets

DESCRIPTION



The purpose of this activity is to create the tables required for the expression of security needs by the users. These will allow users to provide an objective and consistent expression of security needs for elements they normally handle in their work context. This activity assists risk estimation and definition of risk criteria in the risk management process.

PREREQUISITE ACTIVITIES

- Activity 1.2.

INPUTS

- List of issues at stake for the target system.
- List of essential elements

ACTIONS

- Choose the security criteria to be taken into account.
- Determine the scale of needs.
- Determine the relevant impacts.

OUTPUTS

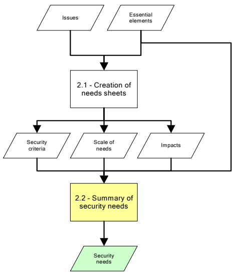
- List of security criteria.
- Scale of needs.
- List of impacts.

PRACTICAL ADVICE

- The scale of needs is one of the most important discussion instruments in the study. It must be determined by the work group and will be used for discussing both security needs and security objectives.
- The scale of needs must be objective and consistent. It must include weightings and reference values and will be based on the list of security criteria to be considered and a list of impacts with representative examples.
- Representation of the impacts in the form of a cause tree provides the work group with a better presentation of the idea.
- To determine their security needs, a sheet must be produced for each essential element and each person interviewed. Creating a sheet for each function or sub-function is justified if the security needs of a function are not directly deduced from the information processed by the function. Examples:
    - A function may be confidential not because it handles confidential information but because of the nature of the processing involved.
    - Access to a service may not necessarily require a high level of availability; however, the operation of this service may necessitate maximum availability of the information it uses.

Activity 2.2 – Summary of security needs

DESCRIPTION



The purpose of this activity is to assign the security needs resulting from the summary of values ascribed by users to the essential elements. This activity will provide an objective and consistent vision of the target system security needs. It contributes to risk evaluation in the risk management process.

PREREQUISITE ACTIVITIES

- ❑ Activity 2.1.

INPUTS

- ❑ List of essential elements.
- ❑ List of security criteria.
- ❑ Scale of needs.
- ❑ List of impacts.

ACTIONS

- ❑ Assign a security need to each essential element taking each security criterion (availability, integrity, confidentiality, etc.) into account.

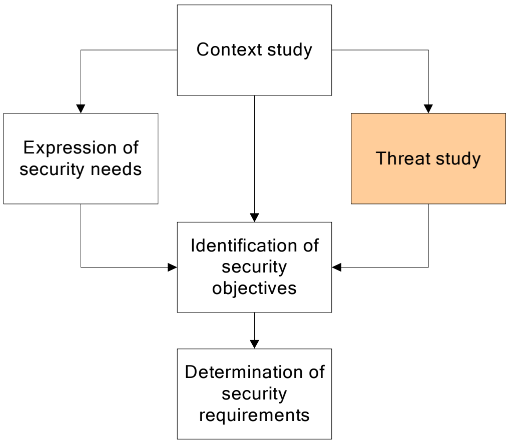
OUTPUTS

- ❑ Security needs summary sheet.

PRACTICAL ADVICE

- ❑ The level of security needs assigned to the essential elements represents the acceptable limit for the organisation.
- ❑ The estimation of security needs represents a user's vision of the system. It is important for the user to justify any extreme values he/she assigns so that the ensuing summary remains consistent across the entire organisation.
- ❑ Wherever possible, all security needs must be justified.
- ❑ The users selected for assessment of security needs must be representative of the use of the system. They must express values for the elements they normally use.
- ❑ The security needs for each essential element can also be added to the functional description by superimposing them on the diagrams. This provides a better understanding of any dependencies between the security need values. There may sometimes be links between security needs for functions and those for information as well as between the functions and data themselves. Security needs may be multiplied if the elements are linked.

Step 3 - Threat study


Context study
Expression of security needs
Threat study
Identification of security objectives
Determination of security requirements

This step contributes to risk assessment. Its purpose is to determine the threats affecting the system.

These threats are formalised by identifying their components: the attack methods to which the organisation is exposed, the threat agents that may use them, the vulnerabilities exploitable on the system entities and their level.

The threats highlighted through this step are specific to the system. Their characterisation is independent of the security needs, information processed and functions supported by the system.

The threat study includes three activities:

- ❑ Study of threat sources
- ❑ Study of vulnerabilities
- ❑ Formalisation of threats

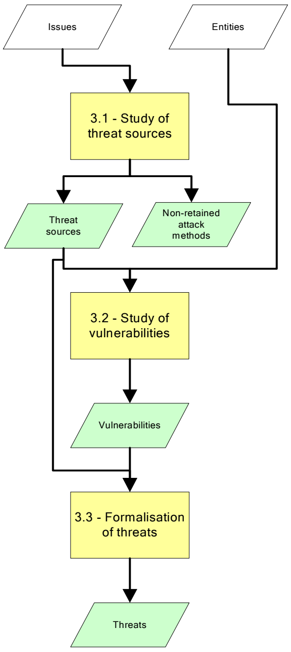
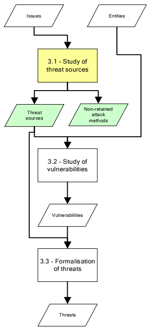

Issues
Entities
3.1 - Study of threat sources
Threat sources
Non-retained attack methods
3.2 - Study of vulnerabilities
Vulnerabilities
3.3 - Formalisation of threats
Threats

Figure 4 - Detailed flowchart of the threat study

Activity 3.1 - Study of threat sources

DESCRIPTION

The purpose of this activity is to select attack methods that are relevant to the target system. Each attack method is characterised by the security criteria it may affect (availability, integrity, confidentiality, etc.) It is associated with threat agents. These threat agents are characterised by their type (natural, human or environmental) and their possible causes (accidental, deliberate). This characterisation may be summarised in the form of an attack potential. If the attack methods constitute real risks for the target system, the level of security measures must be consistent with this attack potential. This activity corresponds to the identification of sources in the risk management process.


Issues
Entities
3.1 - Study of threat sources
Threat sources
Non-retained attack methods
3.2 - Study of vulnerabilities
Vulnerabilities
3.3 - Formalisation of threats
Threats

PREREQUISITE ACTIVITIES

- Activity 1.2.

INPUTS

- List of issues at stake for the target system.

ACTIONS

- List the relevant attack methods.
- Characterise the attack methods according to the security criteria they may breach.
- Characterise the threat agents for each attack method retained, according to their type (natural, human or environmental) and their cause (accidental or deliberate).
- Add a value representing the attack potential of the threat agent.
- Highlight the non-retained attack methods, with justifications.

OUTPUTS

- List of threat sources (attack methods and threat agents).
- List of non-retained threat methods and justifications.

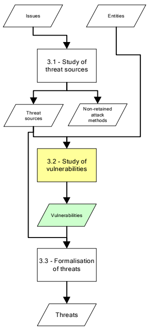
PRACTICAL ADVICE

- It is advisable to use the generic attack methods and threat agents described in the guide "Tools for assessing ISS risks" to list and describe the relevant attack methods and threat agents.
- The attack methods are identified by a security expert working with the manager of the system or missions concerned.
- The justifications used to retain or reject them must be expressed clearly.
- The characterisation of the threat agents should also be expressed in the form of a value representing the attack potential; this value will assist in determining the strength of the mechanisms for the security objectives and requirements.

Activity 3.2 - Study of vulnerabilities

DESCRIPTION

The purpose of this activity is to determine the specific vulnerabilities of the target system and, where appropriate, to characterise them in terms of level. These intrinsic vulnerabilities of the target system arise from the characteristics of the entities it contains. These vulnerabilities can be exploited to attack the security system; the essential purpose of the security objectives will therefore be to reduce them. This activity contributes to risk estimation in the risk management process.


Issues
Entities
3.1 - Study of threat sources
Threat sources
Non-retained attack methods
3.2 - Study of vulnerabilities
Vulnerabilities
3.3 - Formalisation of threats
Threats

PREREQUISITE ACTIVITIES

- Activities 1.3 and 3.1.

INPUTS

- List of entities.
- List of threat sources (attack methods and threat agents).

ACTIONS

- Identify the vulnerabilities of the entities according to attack methods.
- Where appropriate, estimate the level of vulnerabilities.

OUTPUTS

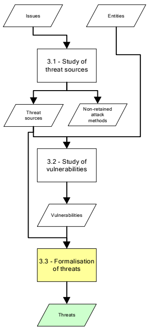
- List of retained vulnerabilities and their level.

PRACTICAL ADVICE

- It is advisable to use the generic vulnerabilities described in the guide "Tools for assessing ISS risks" to identify the vulnerabilities of the entities according to attack methods.
- The study of vulnerabilities is conducted with the same managers involved in the study of threat sources.
- It must be noted that while the proposed list of attack methods is generic in nature and can claim to be exhaustive, the list of vulnerabilities is of a variable nature and must be personalised.

Activity 3.3 – Formalisation of threats

DESCRIPTION


Issues
Entities
3.1 - Study of threat sources
Threat sources
Non-retained attack methods
3.2 - Study of vulnerabilities
Vulnerabilities
3.3 - Formalisation of threats
Threats

The purpose of this activity is to determine the threats that could affect the target system. They result from the linking of attack methods (used by the identified threat agents) with the retained vulnerabilities (based on the identified entities). This activity will provide an objective and exhaustive vision of the threats affecting the target system. This activity contributes to risk estimation in the risk management process.

PREREQUISITE ACTIVITIES

- Activities 3.1 and 3.2.

INPUTS

- List of threat sources (attack methods and threat agents).
- List of retained vulnerabilities and their level.

ACTIONS

- Formulate the threats explicitly.
- Where appropriate, prioritise the threats according to their opportunity.

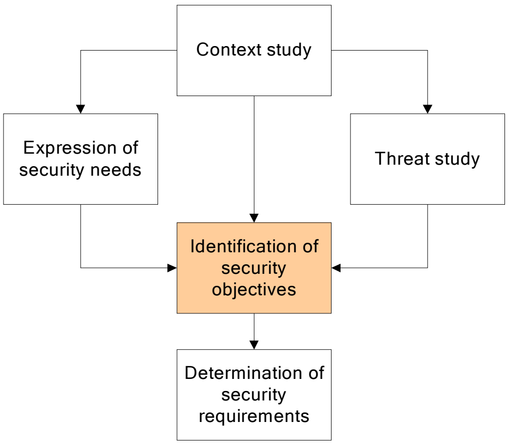
OUTPUTS

- List of retained threats.

PRACTICAL ADVICE

- The formalisation of threats must be as accurate as possible and must highlight the attack method, threat agent, the vulnerability or vulnerabilities exploited and the entities concerned.
- The threats can be characterised by their opportunity, which is determined according to the level of vulnerabilities exploited by the threat agents.

Step 4 – Identification of security objectives


Context study
Expression of security needs
Threat study
Identification of security objectives
Determination of security requirements

The purpose of this step is to evaluate and treat the risks affecting the system.

The comparison of threats with security needs highlights the risks to be covered by the security objectives. These security objectives constitute the security specifications for the target system and its environment. They must be consistent with all the assumptions, constraints, regulatory references and security rules identified during the study.

The level of security objectives and the assurance level must also be determined during this step.

The step includes three activities:

- ❑ Comparison of the threats with the needs
- ❑ Formalisation of security objectives
- ❑ Determination of security levels

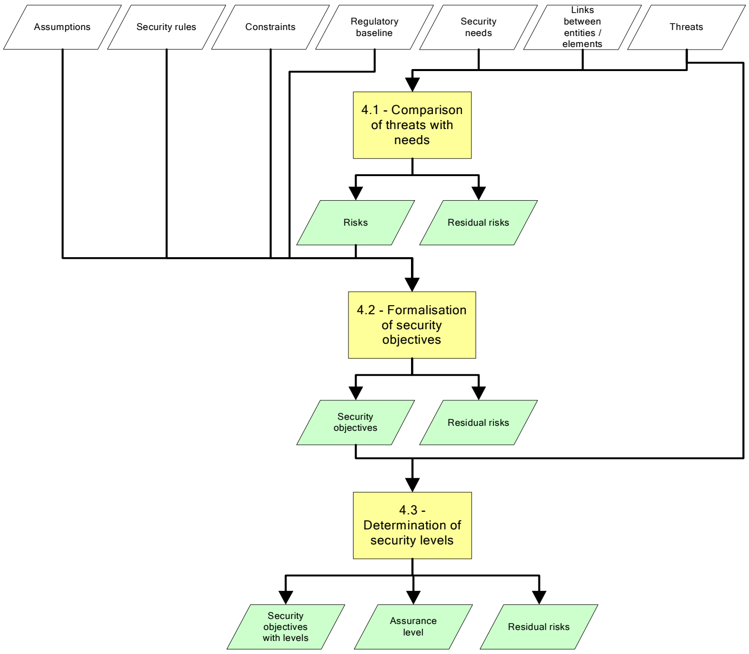
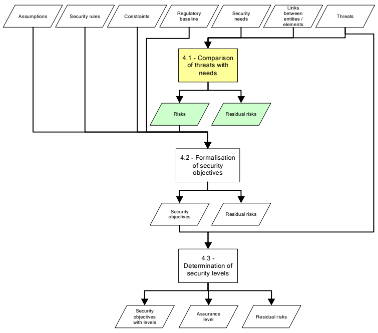

Assumptions
Security rules
Constraints
Regulatory baseline
Security needs
Links between entities / elements
Threats
4.1 - Comparison of threats with needs
Risks
Residual risks
4.2 - Formalisation of security objectives
Security objectives
Residual risks
4.3 - Determination of security levels
Security objectives with levels
Assurance level
Residual risks

Figure 5 - Detailed flowchart of identification of security objectives

Activity 4.1 – Comparison of threats with needs


Assumptions
Security rules
Constraints
Regulatory baseline
Security needs
Links between entities / elements
Threats
4.1 - Comparison of threats with needs
Risks
Residual risks
4.2 - Formalisation of security objectives
Security objectives
Residual risks
4.3 - Determination of security levels
Security objectives with levels
Assurance level
Residual risks

DESCRIPTION

The purpose of this activity is to determine the real risks affecting the target system. By comparing the threats with the security needs, it is possible to decide which risks are genuinely likely to harm the essential elements so that they can be retained and prioritised. All these risks must be evaluated as most of them will need to be covered by security objectives. This activity contributes to risk estimation in the risk management process.

PREREQUISITE ACTIVITIES

- Activities 1.3, 2.2 and 3.3.

INPUTS

- Entity / element tables.
- Security needs summary sheet.
- List of retained threats.

ACTIONS

- Determine the risks by comparing threats with securities needs.
- Formulate the risks explicitly.
- Prioritise the risks according to the impact on the essential elements and the threat opportunity.
- Highlight the non-retained risks (residual risks), with justifications.

OUTPUTS

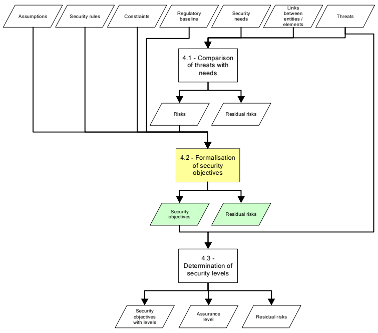
- Prioritised list of risks.
- List of residual risks (risk coverage flaws) and justifications.

PRACTICAL ADVICE

- The more accurate the formulation of a risk, the easier it will be for the reader to understand the risk and for the persons conducting the study to identify accurate and concrete security objectives. The nature of the risk is specific to the target system concerned. The title of a risk may therefore include the threat agent, the vulnerabilities exploited, the entities on which they are based, the essential elements that may be assigned and the possible consequences in terms of security needs and impacts.
- The risks are not prioritised by the persons conducting the study, but by the system users and managers. However, this task will be made easier by the study. For example, the maximum values of security needs that can be affected by the risks and the threat opportunity are used to assess the importance of risks.
- Classification of risks allows priorities to be determined for choosing and implementing countermeasures.

Activity 4.2 – Formalisation of security objectives

DESCRIPTION


Assumptions
Security rules
Constraints
Regulatory baseline
Security needs
Links between entities / elements
Threats
4.1 - Comparison of threats with needs
Risks
Residual risks
4.2 - Formalisation of security objectives
Security objectives
Residual risks
4.3 - Determination of security levels
Security objectives with levels
Assurance level
Residual risks

The purpose of this activity is to determine security objectives to cover the risks at the determined security levels. It must be demonstrated that all risks are fully covered by security objectives, taking into account the assumptions, security rules and constraints. This activity contributes to risk treatment in the risk management process.

PREREQUISITE ACTIVITIES

- ❑ Activities 1.1, 1.2, 2.4 and 4.1.

INPUTS

- ❑ List of assumptions.
- ❑ List of security rules.
- ❑ List of constraints.
- ❑ List of regulatory references.
- ❑ Choice of the security operating mode.
- ❑ Prioritised list of risks.

ACTIONS

- ❑ List the security objectives.
- ❑ Justify the fullness of coverage, checking that the:
  - o risks,
  - o assumptions (and issues at stake),
  - o security rules (and regulatory references),

  are compatible with the constraints affecting the organisation and target system.
- ❑ Where appropriate, classify the security objectives into two categories:
  - o security objectives concerning the target system,
  - o security objectives concerning the target system environment.
- ❑ Highlight the coverage flaws (residual risks), with justifications.

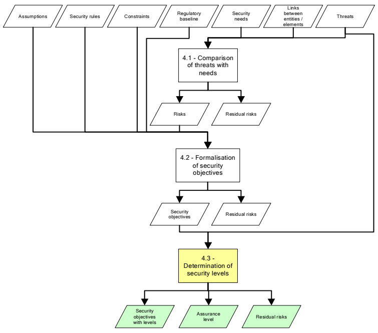
OUTPUTS

- ❑ List of security objectives.
- ❑ List of residual risks (flaw in coverage by security objectives) and justifications.

PRACTICAL ADVICE

- ❑ 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 security objectives can be used as security specifications for which the security solutions allowing the risks to be covered remain open.

Activity 4.3 – Determination of security levels


Assumptions
Security rules
Constraints
Regulatory baseline
Security needs
Links between entities / elements
Threats
4.1 - Comparison of threats with needs
Risks
Residual risks
4.2 - Formalisation of security objectives
Security objectives
Residual risks
4.3 - Determination of security levels
Security objectives with levels
Assurance level
Residual risks

DESCRIPTION

The purpose of this activity is to determine the adequate strength level of the security objectives. It also allows the level of security assurance requirements to be chosen. This activity contributes to risk treatment in the risk management process.

PREREQUISITE ACTIVITIES

- Activities 3.3 and 4.2.

INPUTS

- List of security objectives.
- List of retained threats.

ACTIONS

- Determine the adequate strength level of each security objective.
- Choose the level of assurance requirements.

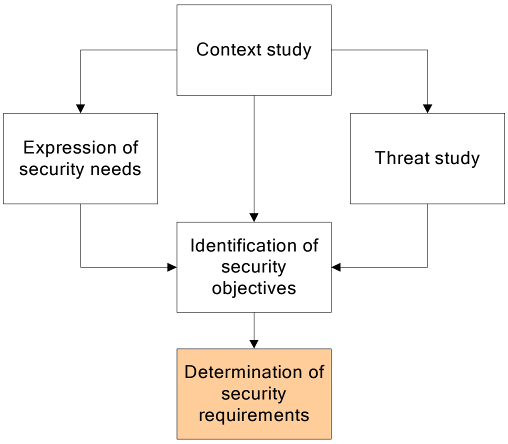
OUTPUTS

- List of security objectives with the strength level.
- List of residual risks (flaw in coverage of strength level by security objectives) and justifications.
- Choice of the level of assurance requirements.

PRACTICAL ADVICE

- The attack potential of the threat agents is used to determine the adequate strength level of the security objectives. This level depends on several factors, including the attack potential, the constraints, the security needs and the threat opportunity.

Step 5 – Determination of security requirements


Context study
Expression of security needs
Threat study
Identification of security objectives
Determination of security requirements

The purpose of this step is to determine how to achieve the security objectives, i.e. how to treat the risks affecting the system.

This requires determining:

- ❑ the security functional requirements describing the required security behaviour and designed to satisfy the security objectives as formulated in the previous step,
- ❑ the security assurance requirements forming the grounds for confidence that the product or system satisfies its security objectives.

These requirements are established especially on the basis of functional and assurance components proposed by [ISO 15408] (Common Criteria).

Coverage of the security objectives by the functional and assurance requirements must be justified by a rationale indicating their necessity and adequacy.

This step includes two main activities:

- ❑ Determination of security functional requirements
- ❑ Determination of security assurance requirements

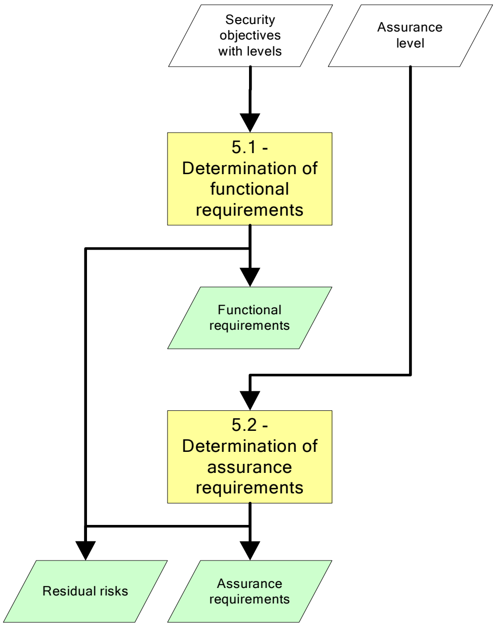
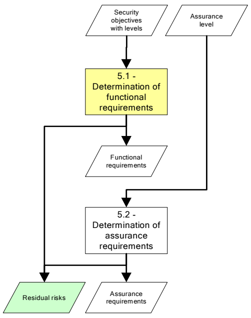

Security objectives with levels
Assurance level
5.1 - Determination of functional requirements
Functional requirements
5.2 - Determination of assurance requirements
Residual risks
Assurance requirements

Figure 6 - Detailed flowchart for determination of security requirements

Article 5.1 - Determination the security functional requirements

DESCRIPTION

The purpose of this activity is to determine the security functional requirements providing adequate coverage of the security objectives identified for the target system. They are used to decide how each identified risk must be treated. The risks may be rejected, optimised, transferred or accepted and the residual risk must be clearly identified and accepted. This activity contributes to risk treatment in the risk management process.


Security objectives with levels
Assurance level
5.1 - Determination of functional requirements
Functional requirements
5.2 - Determination of assurance requirements
Residual risks
Assurance requirements

PREREQUISITE ACTIVITIES

- Activity 4.3.

INPUTS

- List of security objectives with the strength level.

ACTIONS

- List the security functional requirements
- Justify the adequacy of coverage of the security objectives.
- Highlight any coverage flaws (residual risks), with justifications.
- Classify the security functional requirements into two categories:
    - security functional requirements concerning the target system,
    - security functional requirements concerning the target system environment.
- Where appropriate, justify the coverage of dependencies of security functional requirements.

OUTPUTS

- List of justified security functional requirements.
- List of residual risks (flaw in coverage by security functional requirements) and justifications.

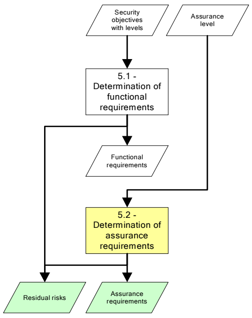
PRACTICAL ADVICE

- 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 designed to satisfy the security objectives covering the vulnerabilities.
- The security functional requirements may be selected from the functional components of the knowledge base or written from scratch. Each of the security objectives must be covered by at least one security requirement and complete coverage must be duly justified. The requirements are then refined, as far as possible, and the dependencies between the components must be studied and justified.
- Depending on the level of expertise on the system, the components may be left unrefined but specifying that they will be refined by the project designer in the context of his reply.

Article 5.2 – Determination of security assurance requirements

DESCRIPTION

The purpose of this activity is to provide a complete expression of the security assurance requirements of the security study target. They are selected according to the assurance level chosen during determination of security levels. They form the grounds for confidence that a target system satisfies its security objectives. This activity contributes to risk treatment in the risk management process.


Security objectives with levels
Assurance level
5.1 - Determination of functional requirements
Functional requirements
5.2 - Determination of assurance requirements
Residual risks
Assurance requirements

PREREQUISITE ACTIVITIES

- ❑ Activity 4.3.

INPUTS

- ❑ Choice of the level of assurance requirements.

ACTIONS

- ❑ List the security assurance requirements
- ❑ Where appropriate, classify the security assurance requirements into two categories:
  - o security assurance requirements concerning the target system,
  - o security assurance requirements concerning the target system environment.
- ❑ Where appropriate, justify the coverage of dependencies of security assurance requirements.

OUTPUTS

- ❑ List of justified security assurance requirements.
- ❑ List of residual risks (flaw in coverage by security assurance requirements) and justifications.

PRACTICAL ADVICE

- ❑ The security assurance requirements may be selected from the functional components of the knowledge base or written from scratch.

Appendix - Data produced

- ❑ Presentation of the organisation.
- ❑ List of general constraints affecting the organisation.
- ❑ List of general regulatory references applicable to the organisation.
- ❑ Conceptual architecture of the information system.
- ❑ Presentation of the target system.
- ❑ List of essential elements.
- ❑ Functional description of the target system.
- ❑ List of issues at stake for the target system.
- ❑ List of assumptions.
- ❑ List of security rules.
- ❑ List of constraints specific to the target system.
- ❑ List of regulatory references specific to the target system.
- ❑ List of entities.
- ❑ Entity / element tables.
- ❑ List of security criteria.
- ❑ Scale of needs.
- ❑ List of impacts.
- ❑ Security needs summary sheet.
- ❑ Choice of the security operating mode.
- ❑ List of threat sources (attack methods and threat agents).
- ❑ List of non-retained threat methods and justifications.
- ❑ List of retained vulnerabilities and their level.
- ❑ List of retained threats.
- ❑ Prioritised list of risks.
- ❑ List of residual risks (risk coverage flaws) and justifications.
- ❑ List of security objectives.
- ❑ List of residual risks (flaw in coverage by security objectives) and justifications.
- ❑ List of security objectives with the strength level.
- ❑ List of residual risks (flaw in coverage of strength level by security objectives) and justifications.
- ❑ Choice of the level of assurance requirements.
- ❑ List of justified security functional requirements.
- ❑ List of residual risks (flaw in coverage by security functional requirements) and justifications.
- ❑ List of justified security assurance requirements.
- ❑ List of residual risks (flaw in coverage by security assurance requirements) and justifications.

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
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