PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

EBIOS®

SECTION 1
INTRODUCTION

Version 2 - 5 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:

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 EBIOS guide	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 requirements scale: 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 attack methods not retained - 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 functional security requirements added to allow functional requirements covering security objectives to be determined and the extent of cover presented - Determination of security requirements for assurance 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

Foreword

The continual search for greater efficiency in accomplishing their mission has led the various government departments to implement means of telecommunications, information technology and office automation. The very widespread use of these technologies makes these organisations dependent on their information systems and therefore vulnerable to the many threats affecting them. This state of affairs contributes considerably to increasing the risks arising from the processing, storing and conveying of information within any organisation.

The new guidelines of the Organisation for Economic Co-operation and Development [OCDE] are being recommended at international level. Their main objective is to promote a "culture of security" as the means of protecting information systems and networks. This means that security must receive very great attention and new ways of thinking and behaving must be adopted during the development and use of information systems and networks. These guidelines comprise nine principles which are complementary and must be considered as a whole.

In our current information society, the purpose of the [eEurope 2005] action plan is to develop on-line public services and high-speed Internet access. Notable examples of its implementation are the modern on-line public services ("e-government", "e-learning", "e-health"), the dynamic electronic business environment ("e-business"), a secure information infrastructure, availability of wide-band access at competitive prices, comparison-based assessment ("benchmarking") and the sharing of good practices.

The French government has committed itself to electronic administration. This means using information technologies in the modernisation of public services and improving the effectiveness of the action of government administrations and local authorities and the quality of relations between them and their users. This computerisation of "public services" cannot be achieved without giving the necessary attention to security. The role of the SGDN DCSSI is to contribute, with the other ministries concerned, to defining and communicating government policy on information systems security.

The government's action may be compromised by the risks arising from the use of information systems. Protection of information and information systems security are therefore major obligations for the nation.

Systems processing classified defence information, are required by [IGI 1300] "to be protected in compliance with a security policy defined according to the level of protection needed, especially the classification level of the processed information, and on the basis of a risk analysis".

This document belongs to a series of methodology guides published by the DCSSI. These are designed to contribute to the improvement of information systems security in public or private organisations. They can be obtained from the DCSSI on request.

They are based on documents that have already been widely discussed within the administration and on the experience and know-how of many industrial companies. The authors believe that the concepts and ideas set out in these documents and methods have been carefully considered and that the selected structure optimises consistency, understanding and ease-of-use.

Note: The references [between square brackets] are presented in the bibliography at the end of the document. The final section also contains a glossary of terms and abbreviations used.

1 Introduction

1.1 The security approach

1.1.1 The security of information systems

Information systems security (ISS) deals first and foremost with information and its "processing". The technical or organisational needs, requirements and objectives derive naturally from these. Three basic criteria must be taken into account: confidentiality, integrity and availability, applying to the information itself and to the systems and environments in which it is found. In some cases it may be necessary to consider the needs of non-repudiation, authorisation and authentication and their coverage by clearly defined audit means.
Assessment and management of risks is an essential part of ISS. These risks are qualified as operational as they directly affect the activities of administrations and companies. Any organisation using means of information and communication technology, especially Internet, to perform its activities and commercial transactions is directly concerned by ISS.

1.1.2 The objects and areas of security

As ISS concerns the information, the processing, the system and its environment, the objects of the security approach will be:

- the information,
- the processes, functions or applications,
- the technology (equipment and operating systems),
- the physical environment (buildings, rooms, etc.),
- the human actors.

All these objects must be clearly defined, remembering that some of them - processes and human actors for example - have special prominence. While each actor may be predominantly involved in one specific area of security, all are involved to some extent in every area.
A security policy that failed to take all these objects and areas into account would be unstable and incomplete. It would produce a dangerous solution based on a false feeling of security even more likely to result in damage than no action at all.

1.1.3 Standardised approaches

Over the past fifteen years or so, a great deal of effort has gone into setting rules, or at least general directives, for managing security of information technologies. This work has resulted in national and international standards such as [ISO 13335], [ISO 17799] etc. Although these standards are still developing and are not yet fully stabilised, they nevertheless provide an important basis.

In France, it is compulsory to write a [FEROS] for systems processing classified defence information, and is recommended in other cases. This statement forms part of the security file used in the system approval procedure.

The international standards make specific information systems security policies subordinate to global policies, which are themselves dependent on information security, the information and communication technologies policy, the personnel policy and the financial and budgetary policy. None of this has any sense unless the actions are defined in compliance with the strategy and general policy of the company or organisation.

The drawing up of the Common Criteria [ISO 15408] encouraged both users and constructors to develop their thinking on information systems security. The Common Criteria are used to assess the assurance level of security-dedicated functions by examining the conformity of their realisation and their effectiveness in countering the identified threats. They were prepared by the DCSSI and its counterpart divisions in Germany, USA, UK, Canada and the Netherlands with the co-operation of European information technology industrialists.

Some international institutions are pushing for standardisation of approaches by publishing specific principles and objectives. These include the principles issued by the OCDE and the directives produced regularly by the European Commission which must be applied by member states. An

example of these principles is that the security approach should be part of the initial planning of a new information system. The design of the information system will then integrate the necessary security elements together with the functional and operational elements, from the start of the project. This guarantees maximum effectiveness, minimum costs and a very positive return on investment. In addition, the security approach should include the complete IS and its environment or its operational context. It should be present at all levels of the organisation and the IS.

1.2 The DCSSI's response

The EBIOS method has been developed in continuity with these approaches and their philosophy. It is generally when the operational master plan for an information system is being prepared. Its main objective is to allow any organisation, including government administrations, to determine the security actions it should undertake.

It can be implemented by the organisation's security expert and can be applied to all levels of an information system structure under design or already in existence (subsystems, applications).

In its first version the EBIOS method was used especially for writing the security objectives [FEROS].
In 2000, taking into account the need to harmonise the writing of protection profiles and basing itself on version 2.0 of the Common Criteria [ISO 15408], the DCSSI began to fit the EBIOS method to these criteria.

The results of an EBIOS study provide the information required for writing the ISS specifications of the system studied (FEROS, protection profile, and so on) and also contribute to preparing the secure operating architecture. For the purposes of a Common Criteria evaluation, the results of the study provide the information required for establishing the specifications of the target of evaluation (they contribute to the development of the security target).

In its essence and general philosophy, the EBIOS approach is also applicable to all levels of the IS - from the global information systems security policy to the specific application - without changing either its formulation or its techniques. It may be useful to may a few vocabulary changes to transpose the concepts of the method to the specific context. For example, the term "function" which appears frequently in the method as an object of the study may be transposed to "job, process, system", etc.
To assist in this transposition and to inform the public concerning the large variety of uses of the EBIOS approach and method, a series of "Best Practices" guides has been developed.

1.3 The method guides

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 functional security objectives and requirements).

This document forms the first section of the method.

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

2 Presentation of the EBIOS method

2.1 What is the EBIOS method?

EBIOS is a French acronym meaning Expression of Needs and Identification of Security Objectives (Expression des Besoins et Identification des Objectifs de Sécurité).

It is not only a **method for assessing ISS risks**, but also a valuable **support tool for the contracting authority** (definition of the scope of study, expression of needs, involvement of the actors, etc.) In conjunction with the Common Criteria and progress in the field of information security management (for example standard [ISO 17799]), EBIOS also becomes a **method for treating ISS risks.**

EBIOS meets the needs of a controlling authority (project leader, contracting authority, system approval authority, management of an organisation, etc.) It allows the security objectives and requirements on the basis of the risks identified and possibly retained.

It constitutes a support in the organisation's perception of security taken in the widest sense of the term. This vision and global approach to security questions provides both an understanding of the existing security provision and also a method for determining a consistent baseline supporting future developments.

2.2 Actions prior to an EBIOS study

Ideally the EBIOS study should be based on the various documents concerning the organisation, its information system and the system to be studied:

- the organisation's master plan;
- the information systems security policy;
- the general specifications of the system (prior to design or installation).

However, it is often the case that these documents are not formalised. The work must therefore begin by collecting the information that must appear in these strategic documents.

A detailed study requires an equal depth of detail in the general system specifications. A system whose objectives are not known cannot be the object of a security study any more than it can be the object of a functional study.

2.3 What is the result of EBIOS?

EBIOS formalises a reasoning process in order to produce the baseline security documents for approval by an authority.

The method allows security objectives and requirements to be identified after assessment of risks and therefore contributes to the production of:

- a master plan for information systems security;
- a security policy;
- an action plan for information systems security;
- a rational expression of security objectives statement [FEROS], regulatory for classified defence systems [IGI 900] and recommended in all other cases, especially those handling sensitive information [REC 901];
- adapted and justified specifications for prime contracting (specification documents);
- a protection profile (PP) or security target (in the sense of [ISO 15408])

EBIOS is also much more:

- a straightforward, flexible and consistent reasoning process;
- a negotiating and decision-making tool in the ISS process;
- a means of unifying vocabulary, concepts and interpretation of the system;
- an approach aiming to make all actors aware, responsible and involved;
- a tool compatible with existing ISS tools ([PSSI], [TDBSSI], [MASSIA], [MAQSSIA], [ISO 15408], [ISO 17799] etc.).

2.4 What the EBIOS method does not provide

The EBIOS study is not a catalogue of ready-to-use security solutions or rules. It is by no means a "black box" with an input and output. It is not therefore a source of intermediate and generic solutions to security problems. It allows security requirements to be determined and appropriate measures to be specified, but these measures will be implemented after the study.

2.5 What the EBIOS method does provide

2.5.1 Assistance for contracting authorities

The EBIOS method assists the preparation of tasks carried out by the contracting authority:

- determining the object of the study through a global vision of the studied system in its context;
- expressing the needs (assets to be protected);
- identifying the threats;
- determining the security actions that need to be undertaken;
- determining the elements that need to be specified when writing [FEROS] or [PP];
- defining a project plan and responsibilities.

2.5.2 A selection and assessment tool for prime contractors

The EBIOS method allows prime contractors to:

- adhere to the objectives expressed by the contracting authority;
- reply to questions concerning feasibility, cost and lead-time;
- select solutions;
- construct security targets.

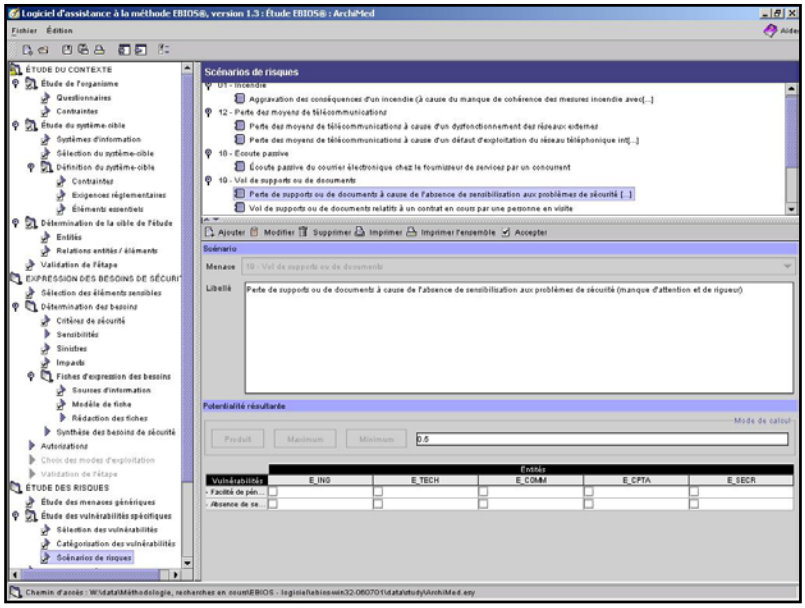
2.5.3 An impact assessment tool assisting negotiations between the contracting authority and management (of the project, organisation, etc.)

The EBIOS method assists management in:

- measuring the impact on the environment;
- checking the suitability of information systems;
- centralising the studies and ISS;
- making strategic decisions concerning security and operations.

3 Tools of the EBIOS method

3.1 Free software



The EBIOS software is an extremely useful support for EBIOS studies. It allows all the study results to be recorded and the required summary documents to be produced. Its intuitive operation allows easy personalisation of knowledge bases.

This software, with its sources, is available free of charge by sending contact details to ebios.dcssi@sgdn.pm.gouv.fr.

It has been developed in Java and XML and can be improved by the user community if feedback is sent to the SGDN.

3.2 Best practices

The EBIOS method provides a range of tools in modular form. The way in which its activities are conducted and the level of detail may vary according to the required deliverable. A collection of best practices has therefore been produced to explain how the results of the EBIOS method should be used according to the required purpose.

- Preparing a master plan for information systems security
- Preparing an information systems security policy
- Writing a FEROS
- Writing an SSRS (*System-specific Requirement Statement* – NATO)
- Writing a protection profile (in compliance with ISO/IEC 15408)
- Writing a security target (in compliance with ISO/IEC 15408)
- Implementation in an information security management context
- Writing a certification policy
- Study prior to system design
- Study of an existing system, etc.

These documents are available on Internet (http://www.ssi.gouv.fr/).

3.3 Training

The CFSSI (training centre of the DCSSI) organises training sessions in the EBIOS method for the French public sector.

The DCSSI also offers instructor training in order to transfer knowledge and avoid any drift in the spread and use of the method.

Information about training can be obtained on the Internet at http://www.ssi.gouv.fr/formation.

3.4 The EBIOS club

A club for major users of the EBIOS method was created in 2003 to bring together a community of experts, share experience and improve the method and its tools.

Glossary

The French translation of the terms in the glossary appears in brackets for each term. The text in italics provides examples. The terms underlined in the definitions are concepts defined in this document.

Asset
(bien)

Any resource of value to the organisation and necessary for achieving its objectives. There is an important distinction between essential elements and entities needing to be protected.

Examples:

- *list of names;*
- *certification request;*
- *invoice management;*
- *encryption algorithm;*
- *laptop computer;*
- *Ethernet;*
- *operating system;*
- *etc.*

Assumption
(hypothèse)

Supposition concerning the operational environment of the system, applied to obtain the required security functionalities.

Examples:

- *the system will be installed in a room designed to minimise electromagnetic emanation;*
- *the administrator will occupy a restricted access area;*
- *users will not write down their passwords;*
- *the network will not be connected to a network that has not been proved to be trustworthy;*
- *everyone in the company knows their responsibilities concerning illicit release of professional information or illegal manipulation of personal data;*
- *etc.*

Attack
(attaque)

Exploiting one or more vulnerabilities using an attack method with a given opportunity.

Examples:

- *strong opportunity of using counterfeit or copied software resulting from total absence of awareness or information concerning copyright legislation;*
- *software damaged by a virus through easy loading of malicious programmes onto the organisation's office network;*
- *etc.*

Attack method
(méthode d'attaque)

Standard means (action or event) by which a threat agent carries out an attack.

Examples:

- *theft of media or documents;*
- *software entrapment;*
- *attack on availability of personnel;*
- *passive wiretapping;*
- *flood;*
- *…*

Availability
(disponibilité)

Property of essential elements that allows authorised users to access them at the required time.

Available resources
(ressources disponibles)

Expected means of a threat agent. The level of available resources constitutes its attack potential and can be characterised as low, moderate or high.

Examples:

- *low resources;*
- *moderate resources;*
- *high resources.*

Confidentiality
(confidentialité)

Property of essential elements making them only accessible to authorised users.

Entity
(entité)

An asset such as an organisation, site, personnel, equipment, network, software, system.

Examples:

- *facilities management company;*
- *the organisation's premises;*
- *system administrator;*
- *laptop computer;*
- *Ethernet;*
- *operating system;*
- *teleprocedure gateway;*
- *…*

Essential element
(élément essentiel)

Information or function with at least one non-nil sensitivity.

Examples:

- *list of names;*
- *certification request;*
- *invoice management;*
- *encryption algorithm;*
- *etc.*

Expertise
(expertise)

Expected level of technical competence of a threat agent with a premeditated motive. This level can be characterised by low, medium or high technical competence.

Examples [Guide 650]:

- *low technical competence;*
- *medium technical competence;*
- *high technical competence.*

Exposure
(exposition)

Level of natural exposure of a target system to a threat agent with an accidental cause. This level may be characterised as low, moderate or high exposure.

Examples:

- *low exposure;*
- *moderate exposure;*
- *high exposure.*

Function
(fonction)

Process or set of processes contributing to the operation of an activity of an organisation which creates, modifies, destroys or conveys information.

Examples:

- *creating technical drawings;*
- *drawing up an estimate;*
- *invoice management;*
- *an encryption algorithm;*
- *generating a certificate;*
- *etc.*

Impact
(impact)

Consequences for an organisation when a threat is accomplished.

Examples:

- *loss of customers' confidence in a trade mark;*
- *financial loss of 10% of turnover;*
- *infringement of laws and regulations leading to legal proceedings against the Director;*
- *etc.*

Information
(information)

Information or item of knowledge that can be represented in a form allowing its communication, recording or processing. [IGI 900] [REC 901]

Examples:

- *a message;*
- *list of names;*
- *certification request;*
- *revocation list;*
- *etc.*

Information system (IS)
(système d'information)

All entities organised to accomplish the information processing functions.

Information systems security (ISS)
(sécurité des systèmes d'information (SSI))

Protection of information systems and especially essential elements, against any unauthorised violation of the security criteria, whether accidental or deliberate.

Information systems security policy
(politique de sécurité de système d'information)

Set of strategic information, directives, procedures, codes of conduct, organisational and technical rules formalised in an applicable document whose objective is to protect the organisation's information system(s).

Integrity
(intégrité)

Property defining the accuracy and completeness of the essential elements.

Motivation
(motivation)

Motive of a threat agent. It may arise from strategy, ideology, terrorism, greed, amusement or revenge and may be an accidental action (arising from curiosity, boredom, etc.) or a deliberate action (arising from spying, the lure of gain, the intention to harm, ideology, amusement, fraud, theft, piracy, intellectual challenge, revenge, blackmailing, extortion of money, etc.)

Examples [Guide 650]:

- *motivated by strategy;*
- *motivated by ideology;*
- *motivated by terrorism;*
- *motivated by greed;*
- *motivated by amusement;*

- *motivated by revenge;*

[etc.]

- *in the case of a deliberate act:*
  - *spying,*
  - *lure of gain,*
  - *intention to harm,*
  - *ideology,*
  - *amusement,*
  - *fraud,*
  - *theft,*
  - *piracy,*
  - *intellectual challenge,*
  - *revenge,*
  - *blackmail,*
  - *extortion of money,*
  - *…*
- *in the case of an accidental act:*
  - *curiosity*
  - *boredom,*
  - *etc.*

Opportunity
(opportunité)

Level of possibility of an attack occurring.

Examples:

- *unlikely;*
- *highly likely;*
- *totally unfeasible;*
- *15% chance of occurring;*
- *…*

Organisational security policy
(règle de sécurité)

Security rule, procedure, code of conduct or guideline that an organisation imposes for its operation. [ISO 15408]

Examples:

- *all products used by the government must comply with national standards for password generation and cryptology;*
- *all products used in the field of banking must be certified to level EAL4 increased by the ADV_IMP.2 component;*
- *access is controlled by identifier / password;*
- *each engineer is responsible for the file he processes;*
- *an intrusion alarm is active during closed hours (19.00 - 07.00);*
- *…*

Residual risk
(risque résiduel)

Risk that persists after risk treatment. [ISO Guide 73]

Risk
(risque)

Combination of a threat and the losses it can cause, i.e.: of the opportunity, for a threat agent using an attack method, to exploit one or more vulnerabilities of one or more entities and the impact on the essential elements and on the organisation.

Examples:

- *a former member of the personnel with little technical ability but possibly strong motivation, deliberately damages the system software by introducing a virus, taking advantage of the ease of installing harmful programmes on the organisation's office network; this could affect, for example, the functions generating estimates or signature certificates, which could result in the inability to provide a service, impossibility of fulfilling contractual obligations and serious consequences in terms of confidence in a trade mark;*
- *a cracker with a good level of expertise, standard equipment*

and paid for his actions, steals confidential files by remotely accessing the company's network, causing a transaction with a partner to fail and loss of customers' confidence;
- *…*

Risk acceptance (acceptation du risque)
Decision to accept a risk treated according to the risk criteria.

Risk analysis (analyse du risque)
Systematic use of data to identify the sources of attacks and estimate the risk.

Risk assessment (appréciation du risque)
The complete process combining risk analysis and risk evaluation. [ISO Guide 73]

Risk communication (communication relative au risque)
Exchange or sharing of information concerning the risk between the decision-maker and other parties involved. [ISO Guide 73]

Risk criteria (critères de risque)
Reference terms allowing the importance of risks to be assessed.

Risk estimation (estimation du risque)
Process used to assign values to the opportunity and losses that a risk could create.

Risk evaluation (évaluation du risque)
Process of comparing the estimated risk with the given risk criteria to determine the size of a risk. [ISO Guide 73]

Risk management (gestion du risque)
Co-ordinated activities aimed at directing or guiding an organisation's response to the risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication. [ISO Guide 73]

Risk reduction (réduction du risque)
Process aiming to minimise the negative consequences and opportunities of a threat.

Risk retention (prise de risque)
Acceptance of the possible loss associated with a particular risk.

Risk transfer (transfert du risque)
Sharing with another party the possible loss associated with a particular risk.

Examples:
- *taking out an insurance policy;*
- *etc.*

Security assurance requirement (exigence d'assurance de sécurité)
Specification of the assurance provided by security functions to be implemented to contribute to one or more security objectives, and generally concerning the system development environment.

Examples:
- *the developer must provide functional specifications;*
- *the functional specifications must describe the purpose and operating instructions of all external interfaces of security functions, by providing, where appropriate, full details concerning all the effects, the exceptions and the error messages;*
- *the elements of proof must show that the security measures provide the protection level needed for maintaining the confidentiality and integrity of the system;*
- *…*

Security criterion — Characteristic of an essential element allowing the various sensitivities to be assessed.

Security functional requirement (exigence fonctionnelle de sécurité) — Functional specification of the security functions to be implemented to contribute to covering one or more security objectives for the target system.

Examples:

- *the system must generate the encryption keys in compliance with a specified encryption key generation algorithm and with the specified sizes of encryption keys in compliance with specified standards;*
- *the system must unambiguously detect a physical intrusion that could compromise it;*
- *a lightning conductor must be installed at the organisation's premises;*
- *etc.*

Security measure (mesure de sécurité) — A measure designed to improve security, specified by a security requirement and implemented to comply with it. The effect of the measures may be to anticipate, prepare, dissuade, protect, detect, confine, combat, recover, restore, compensate, etc.

Security objective (objectif de sécurité) — Expression of the intention to counter identified threats or risks (depending on the context) and/or comply with the organisational security policies and assumptions; an objective can concern the target system, its development environment or its operational environment.

Examples:

- *"open" objectives (security objective can be covered by a wide range of means):*
  - *the configuration of internal network stations must be upgradable;*
  - *the rooms must be protected against lightning;*
  - *…*
- *"closed" objectives (security objective can only be covered by a narrow range of means):*
  - *the system must allow unique identification and authentication of users before any interaction between the system and the user;*
  - *two different and compatible antivirus programmes must be installed and the signature bases updated every two weeks;*
  - *…*

Security principle (principe de sécurité) — The security principles are the expression of the necessary security orientations and major security characteristics for preparing a policy and especially the security rules that constitute it.

Security requirement (exigence de sécurité) — Functional or assurance specification concerning the information system or the its environment, dealing with the security mechanisms to be implemented and covering one or more security objectives.

Sensitivity — Precise and unambiguous definition of levels corresponding to

(besoin de sécurité)	security criteria (availability, confidentiality, integrity etc.) which must be provided for an essential element.
Source identification (identification des origines des attaques)	Process allowing the sources of attacks (threat agents and attack methods) to be found, assessed and characterised.
Threat (menace)	Possible attack of a threat agent on assets. *Examples:* - *a former member of the personnel with little technical ability but possibly a strong motivation to carry out an attack deliberately damages the system software by introducing a virus, taking advantage of the ease of installing harmful programmes on the organisation's office network; this could affect, for example, the functions generating estimates or signature certificates;* - *a cracker with a good level of expertise, standard equipment and paid for his actions, steals confidential files by remote access to the company's network;* - *a developer or member of the personnel with a very good level of expertise in source codes but little ISS knowledge deliberately modifies the source code;* - *a visitor steals equipment containing confidential information;* - *etc.*
Threat agent (élément menaçant)	Human action, natural or environmental element that has potentially negative consequences on the system. It can be characterised by its type (natural, human or environmental) and by its cause (accidental or deliberate). In the case of an accidental cause, it is also characterised by exposure and available resources. In the case of a deliberate cause, it is also characterised by expertise, available resources and motivation. *Examples:* - *former member of the personnel with little technical ability and time but possibly a strong motivation to carry out an attack;* - *cracker with considerable technical ability, well equipped and strongly motivated by the money he could make;* - *very wet climate for three months of the year;* - *virus;* - *users;* - *developers;* - *etc.*
User (utilisateur)	Person or object that uses an organisation's services.
Vulnérability (vulnerabilité)	Characteristic of an entity that can constitute a weakness or flaw in terms of information systems security. *Examples:* - *no fire safety arrangements for an Organisation type entity;* - *little attention drawn to security problems for a Personnel type entity;* - *ease of intrusion into site for a Site type entity;* - *possibility of creating or modifying system commands for a Network type entity;* - *etc.*
Risk acceptance (acceptation du risque)	Decision to accept a risk treated according to the risk criteria.

Risk analysis (analyse du risque)	Systematic use of data to identify the sources of attacks and estimate the risk.
Risk assessment (appréciation du risque)	The complete process combining risk analysis and risk evaluation. [ISO Guide 73]
Attack (attaque)	Exploiting one or more vulnerabilities using an attack method with a given opportunity. *Examples:* - *strong opportunity of using counterfeit or copied software resulting from total absence of awareness or information concerning copyright legislation;* - *software damaged by a virus through easy loading of malicious programmes onto the organisation's office network;* - *etc.*
Sensitivity (besoin de sécurité)	Precise and unambiguous definition of levels corresponding to security criteria (availability, confidentiality, integrity etc.) which must be provided for an essential element.
Asset (bien)	Any resource of value to the organisation and necessary for achieving its objectives. There is an important distinction between essential elements and entities needing to be protected. *Examples:* - *list of names;* - *certification request;* - *invoice management;* - *encryption algorithm;* - *laptop computer;* - *Ethernet;* - *operating system;* - *etc.*
Risk communication (communication relative au risque)	Exchange or sharing of information concerning the risk between the decision-maker and other parties involved. [ISO Guide 73]
Confidentiality (confidentialité)	Property of essential elements making them only accessible to authorised users.

Security criterion — Characteristic of an essential element allowing the various sensitivities to be assessed.

Risk criteria (critères de risque) — Reference terms allowing the importance of risks to be assessed.

Availability (disponibilité) — Property of essential elements that allows authorised users to access them at the required time.

Essential element (élément essentiel) — Information or function with at least one non-nil sensitivity.

Examples:

- *list of names;*
- *certification request;*
- *invoice management;*
- *encryption algorithm;*
- *etc.*

Threat agent (élément menaçant) — Human action, natural or environmental element that has potentially negative consequences on the system. It can be characterised by its type (natural, human or environmental) and by its cause (accidental or deliberate). In the case of an accidental cause, it is also characterised by exposure and available resources. In the case of a deliberate cause, it is also characterised by expertise, available resources and motivation.

Examples:

- *former member of the personnel with little technical ability and time but possibly a strong motivation to carry out an attack;*
- *cracker with considerable technical ability, well equipped and strongly motivated by the money he could make;*
- *very wet climate for three months of the year;*
- *virus;*
- *users;*
- *developers;*
- *etc.*

Entity (entité) — An asset such as an organisation, site, personnel, equipment, network, software, system.

Examples:

- *facilities management company;*
- *the organisation's premises;*
- *system administrator;*
- *laptop computer;*
- *Ethernet;*
- *operating system;*
- *teleprocedure gateway;*
- *…*

Risk estimation (estimation du risque) — Process used to assign values to the opportunity and losses that a risk could create.

Risk evaluation (évaluation du risque) — Process of comparing the estimated risk with the given risk criteria to determine the size of a risk. [ISO Guide 73]

Security assurance requirement
(exigence d'assurance de sécurité)

Specification of the assurance provided by security functions to be implemented to contribute to one or more security objectives, and generally concerning the system development environment.

Examples:

- *the developer must provide functional specifications;*
- *the functional specifications must describe the purpose and operating instructions of all external interfaces of security functions, by providing, where appropriate, full details concerning all the effects, the exceptions and the error messages;*
- *the elements of proof must show that the security measures provide the protection level needed for maintaining the confidentiality and integrity of the system;*
- *…*

Security requirement
(exigence de sécurité)

Functional or assurance specification concerning the information system or the its environment, dealing with the security mechanisms to be implemented and covering one or more security objectives.

Security functional requirement
(exigence fonctionnelle de sécurité)

Functional specification of the security functions to be implemented to contribute to covering one or more security objectives for the target system.

Examples:

- *the system must generate the encryption keys in compliance with a specified encryption key generation algorithm and with the specified sizes of encryption keys in compliance with specified standards;*
- *the system must unambiguously detect a physical intrusion that could compromise it;*
- *a lightning conductor must be installed at the organisation's premises;*
- *etc.*

Expertise
(expertise)

Expected level of technical competence of a threat agent with a premeditated motive. This level can be characterised by low, medium or high technical competence.

Examples [Guide 650]:

- *low technical competence;*
- *medium technical competence;*
- *high technical competence.*

Exposure
(exposition)

Level of natural exposure of a target system to a threat agent with an accidental cause. This level may be characterised as low, moderate or high exposure.

Examples:

- *low exposure;*
- *moderate exposure;*
- *high exposure.*

Function
(fonction)

Process or set of processes contributing to the operation of an activity of an organisation which creates, modifies, destroys or conveys information.

Examples:

- *creating technical drawings;*
- *drawing up an estimate;*
- *invoice management;*
- *an encryption algorithm;*
- *generating a certificate;*
- *etc.*

Risk management
(gestion du risque)

Co-ordinated activities aimed at directing or guiding an organisation's response to the risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication. [ISO Guide 73]

Assumption
(hypothèse)

Supposition concerning the operational environment of the system, applied to obtain the required security functionalities.

Examples:

- *the system will be installed in a room designed to minimise electromagnetic emanation;*
- *the administrator will occupy a restricted access area;*
- *users will not write down their passwords;*
- *the network will not be connected to a network that has not been proved to be trustworthy;*
- *everyone in the company knows their responsibilities concerning illicit release of professional information or illegal manipulation of personal data;*
- *etc.*

Source identification
(identification des origines des attaques)

Process allowing the sources of attacks (threat agents and attack methods) to be found, assessed and characterised.

Impact
(impact)

Consequences for an organisation when a threat is accomplished.

Examples:

- *loss of customers' confidence in a trade mark;*
- *financial loss of 10% of turnover;*
- *infringement of laws and regulations leading to legal proceedings against the Director;*
- *etc.*

Information
(information)

Information or item of knowledge that can be represented in a form allowing its communication, recording or processing. [IGI 900] [REC 901]

Examples:

- *a message;*
- *list of names;*
- *certification request;*
- *revocation list;*
- *etc.*

Integrity
(intégrité)

Property defining the accuracy and completeness of the essential elements.

Threat
(menace)

Possible attack of a threat agent on assets.

Examples:

- *a former member of the personnel with little technical ability but possibly a strong motivation to carry out an attack deliberately damages the system software by introducing a virus, taking advantage of the ease of installing harmful programmes on the organisation's office network; this could affect, for example, the functions generating estimates or signature certificates;*
- *a cracker with a good level of expertise, standard equipment and paid for his actions, steals confidential files by remote access to the company's network;*
- *a developer or member of the personnel with a very good level of expertise in source codes but little ISS knowledge deliberately modifies the source code;*
- *a visitor steals equipment containing confidential information;*
- *etc.*

Security measure
(mesure de sécurité)

A measure designed to improve security, specified by a security requirement and implemented to comply with it. The effect of the measures may be to anticipate, prepare, dissuade, protect, detect, confine, combat, recover, restore, compensate, etc.

Attack method
(méthode d'attaque)

Standard means (action or event) by which a threat agent carries out an attack.

Examples:

- *theft of media or documents;*
- *software entrapment;*
- *attack on availability of personnel;*
- *passive wiretapping;*
- *flood;*
- *…*

Motivation
(motivation)

Motive of a threat agent. It may arise from strategy, ideology, terrorism, greed, amusement or revenge and may be an accidental action (arising from curiosity, boredom, etc.) or a deliberate action (arising from spying, the lure of gain, the intention to harm, ideology, amusement, fraud, theft, piracy, intellectual challenge, revenge, blackmailing, extortion of money, etc.)

Examples [Guide 650]:

- *motivated by strategy;*
- *motivated by ideology;*
- *motivated by terrorism;*
- *motivated by greed;*
- *motivated by amusement;*
- *motivated by revenge;*

[etc.]

- *in the case of a deliberate act:*
  - *spying,*
  - *lure of gain,*
  - *intention to harm,*
  - *ideology,*
  - *amusement,*
  - *fraud,*
  - *theft,*
  - *piracy,*
  - *intellectual challenge,*
  - *revenge,*
  - *blackmail,*

- *extortion of money,*
- *…*

- *in the case of an accidental act:*
  - *curiosity*
  - *boredom,*
  - *etc.*

Security objective
(objectif de sécurité)

Expression of the intention to counter identified threats or risks (depending on the context) and/or comply with the organisational security policies and assumptions; an objective can concern the target system, its development environment or its operational environment.

Examples:

- *"open" objectives (security objective can be covered by a wide range of means):*
  - *the configuration of internal network stations must be upgradable;*
  - *the rooms must be protected against lightning;*
  - *…*
- *"closed" objectives (security objective can only be covered by a narrow range of means):*
  - *the system must allow unique identification and authentication of users before any interaction between the system and the user;*
  - *two different and compatible antivirus programmes must be installed and the signature bases updated every two weeks;*
  - *…*

Opportunity
(opportunité)

Level of possibility of an attack occurring.

Examples:

- *unlikely;*
- *highly likely;*
- *totally unfeasible;*
- *15% chance of occurring;*
- *…*

Information systems security policy
(politique de sécurité de système d'information)

Set of strategic information, directives, procedures, codes of conduct, organisational and technical rules formalised in an applicable document whose objective is to protect the organisation's information system(s).

Security principle
(principe de sécurité)

The security principles are the expression of the necessary security orientations and major security characteristics for preparing a policy and especially the security rules that constitute it.

Risk retention
(prise de risque)

Acceptance of the possible loss associated with a particular risk.

Risk reduction
(réduction du risque)

Process aiming to minimise the negative consequences and opportunities of a threat.

Organisational security policy
(règle de sécurité)

Security rule, procedure, code of conduct or guideline that an organisation imposes for its operation. [ISO 15408]

Examples:

- *all products used by the government must comply with national standards for password generation and cryptology;*
- *all products used in the field of banking must be certified to level EAL4 increased by the ADV_IMP.2 component;*
- *access is controlled by identifier / password;*
- *each engineer is responsible for the file he processes;*
- *an intrusion alarm is active during closed hours (19.00 - 07.00);*
- *…*

Available resources
(ressources disponibles)

Expected means of a threat agent. The level of available resources constitutes its attack potential and can be characterised as low, moderate or high.

Examples:

- *low resources;*
- *moderate resources;*
- *high resources.*

Risk
(risque)

Combination of a threat and the losses it can cause, i.e.: of the opportunity, for a threat agent using an attack method, to exploit one or more vulnerabilities of one or more entities and the impact on the essential elements and on the organisation.

Examples:

- *a former member of the personnel with little technical ability but possibly strong motivation, deliberately damages the system software by introducing a virus, taking advantage of the ease of installing harmful programmes on the organisation's office network; this could affect, for example, the functions generating estimates or signature certificates, which could result in the inability to provide a service, impossibility of fulfilling contractual obligations and serious consequences in terms of confidence in a trade mark;*
- *a cracker with a good level of expertise, standard equipment and paid for his actions, steals confidential files by remotely accessing the company's network, causing a transaction with a partner to fail and loss of customers' confidence;*
- *…*

Residual risk
(risque résiduel)

Risk that persists after risk treatment. [ISO Guide 73]

Information systems security (ISS)
(sécurité des systèmes d'information (SSI))

Protection of information systems and especially essential elements, against any unauthorised violation of the security criteria, whether accidental or deliberate.

Information system (IS)
(système d'information)

All entities organised to accomplish the information processing functions.

Risk treatment
(traitement du risque)

Process for selecting and implementing measures aimed at modifying the risk, i.e. risk reduction, risk transfer or risk retention.

Risk transfer
(transfer du risque)

Sharing with another party the possible loss associated with a particular risk.

Examples:

- *taking out an insurance policy;*
- *etc.*

User
(utilisateur)

Person or object that uses an organisation's services.

Vulnérability
(vulnerabilité)

Characteristic of an entity that can constitute a weakness or flaw in terms of information systems security.

Examples:

- *no fire safety arrangements for an Organisation type entity;*
- *little attention drawn to security problems for a Personnel type entity;*
- *ease of intrusion into site for a Site type entity;*
- *possibility of creating or modifying system commands for a Network type entity;*
- *etc.*

Acronyms

BCS	Advisory Office for Information Systems Security (Bureau Conseil en Sécurité des systèmes d'information)
CC	Common Criteria - the title used for some time to refer to the standard instead of the official ISO title: "Evaluation criteria for information technology security"
CFSSI	Training centre for information systems security (Centre de Formation en Sécurité des Systèmes d'Information)
DCSSI	Central information systems security division (Direction Centrale de la Sécurité des Systèmes d'Information)
EBIOS	Expression of needs and identification of security objectives (Expression des Besoins et Identification des Objectifs de Sécurité)
FEROS	Rational expression of security objectives statement (Fiche d'Expression Rationnelle des Objectifs de Sécurité des SI)
PP	Protection profile
PSSI	Information systems security policy (Politique de Sécurité des Systèmes d'Information)
SDO	Operations subdivision (Sous-Direction des Opérations)
SDSSI	Information systems security master plan (Schéma Directeur de la Sécurité des Systèmes d'Information(
SGDN	General secretariat of national defence (Secrétariat Général de la Défense Nationale)
SI	Information system (Système d'Information)
ISS	Information systems security
TIC	Information and communication technologies (Technologies de l'Information et de Communication)

Reference documents

[eEurope 2005] *Plan d'action eEurope 2005 : une société de l'information pour tous, COM(2002)263 final* – Commission européenne (2002).

[FEROS] *Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS)* – SGDN/SCSSI (1991).

Avalaible on the following site http://www.ssi.gouv.fr

[Guide 650] *La menace et les attaques informatiques* – N°650 / DISSI / SCSSI (1994).

Avalaible on the following site http://www.ssi.gouv.fr

[IGI 1300] *Instruction générale interministérielle sur la protection du secret de la défense nationale* – N°1300 / SGDN / PSE / SSD (2003).

[IGI 900] *La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées* – SGDN et DISSI (1993).

[ISO 13335] *Information technology – Security techniques – Guidelines for the management of IT security (GMITS)* – International Organization for Standardization (ISO) (2001).

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information*, – International Organization for Standardization (ISO) – version 2.0 (1998).

[ISO 17799] *Information technology – Code of practice for information security management* – International Organization for Standardization (ISO) (2000).

[ISO Guide 73] *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes* – International Organization for Standardization (ISO) (2002).

[MASSIA] *Méthode d'Audit de la Sécurité des Systèmes d'Information de l'Armement* – CELAR/CASSI/GESSI – version 1.0 (1994).

[OCDE] *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* – Organisation de coopération et de développement économiques (OCDE) (2002).

[PSSI] *Guide d'élaboration de politique de sécurité de système d'information* – DCSSI (2004).

Avalaible on the following site http://www.ssi.gouv.fr

[REC 901] *Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense* – SGDN et DISSI (1994).

TDBSSI *Guide d'élaboration de tableaux de bord de sécurité de système d'information pour les administrations* – DCSSI (2004).

Avalaible on the following site http://www.ssi.gouv.fr

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