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

EBIOS

MEMO

4 March 2004

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

Why does EBIOS enjoy such success?

A reference among ISS risk analysis methods

The methodological approach offered by EBIOS provides **a global and consistent view** of information systems security (ISS). It provides uniform vocabulary and concepts and allows exhaustive coverage with determination of suitable security objectives and requirements. The method takes into account all technical entities (software, hardware, networks) and non-technical entities (organisation, human aspects, physical safety). It allows all personnel using the IS to be involved in security issues and offers a dynamic approach that encourages interaction between the organisation's various jobs and functions by examining the complete life cycle of the system (design, production, implementation, maintenance, etc.).

Promoted by the DCSSI and **recognised by the French administrations, EBIOS is also a reference in the private sector and abroad.** In this context, its translation into English and harmonisation with international standards open new opportunities. In 2002, international comparisons placed EBIOS among the three best methods for analysing ISS risks.

Many organisations in the public and private sectors use the method **to conduct their own ISS risk analyses:** administrations (used systematically by some, encouraged by others), the National Centre for Space Studies (CNES), the French Atomic Energy Commission (CEA), the National Health Insurance Fund (CNAM), the CB Bank Card Group, ALCATEL CIT, health agencies, Paris Airports (ADP), the Council of the European Union, etc.

In addition, **several consulting firms have adopted the EBIOS approach** in the support they provide to contracting authorities.

Finally, we should remember that a ministry or manufacturer must write a FEROS (Rational expression of security objectives statement - Fiche d'Expression Rationnelle des Objectifs de Sécurité) whenever a system processes defence classified information. EBIOS is an ideal tool for this work because its results can be directly incorporated into a FEROS.

A straightforward approach with specific results

The EBIOS method is **easy to understand and apply.** Its overall philosophy is straightforward and intuitive and it follows a natural sequence. It consists in formalising the sensitivities and threats and determining the associated risks for the organisation.

Any user can grasp the method and adapt its approach to the subjects studied. EBIOS has been applied both to basic systems (Web server) and to complex systems (human resources management system interconnecting several elements), at the pre-design stage or on existing systems, to complete information systems or to subsystems.

One and the same tool is used to carry out the various security operations linked to ISS risk management. EBIOS is used to assist preparation of an ISS master plan, to carry out the first steps of an ISS policy and produce an ISS trend chart, to assist the writing of a Protection Profile (PP), or a FEROS, or any other ISS specifications.

The EBIOS method contributes to the preparation of the contracting authority's tasks. It is used to determine the scope of study while maintaining a global view of the system in its context, to express needs (linked to the assets to be protected), to identify threats and to define a project plan and responsibilities.

The EBIOS method is a selection and assessment tool for prime contractors enabling them to adhere to the objectives expressed by the contracting authority, answer questions concerning feasibility, costs and lead-times and, finally, select solutions.

It is also an impact assessment tool assisting negotiations between the contracting authority and management (of the project, organisation, etc.) allowing the management team to check the adequacy of information systems and centralise the studies and ISS.

Its **compatibility with other ISS methodology tools** ensures that the ISS risk management process remains perfectly consistent. For example, ISO/IEC 15408 and ISO/IEC 17799 can be used to determine the security objectives and requirements.

A support application under freeware licence

The software is free and available on request from the DCSSI (conseil.dcssi@sgdn.pm.gouv.fr). Its intuitive approach **makes risks analyses much easier to carry out** and offers the possibility of preparing various analysis documents (complete data, FEROS, FEROS summary, PP, identification of strategic elements, security policy, etc.). In addition, it allows knowledge bases and studies to reused. The software is delivered with its sources and design documents and can be improved by any user. It is published under a freeware licence, designed in UML and coded in Java and XML.

A strong demand for training

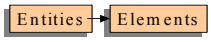
The EBIOS training session makes the method and its application easier to understand. It familiarises trainees with good implementation practices and allows them to discuss issues with users of the method. This two-day training session is held at the CFSSI (http://www.ssi.gouv.fr/formation/index.html). A case study provides a concrete illustration of the approach and examples that can be referred to during initial use of the method.
A session has also been set up for instructors of the EBIOS method, with the aim of creating information relays inside administrations.

The EBIOS club

The EBIOS club was created by the DCSSI in 2003 to share experience and improve the method and its tools.

It is a regular meeting place for a community of users keen to contribute to the development of the method and obtain the latest information about it.

The principles of the EBIOS method



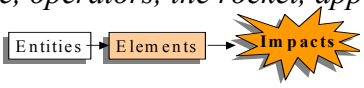
The context study

An information system is based on **essential elements**, functions and information which constitute the added value of the information system for the organisation.

For example, a system monitoring a rocket launch trajectory relies on various information such as parameters or computation results and on various functions allowing this computation to be carried out.

The essential elements are linked to a set of **entities** of various types: hardware, software, networks, organisations, personnel and sites.

Let us take the example of a parameter used to compute the rocket launch trajectory. It is linked to the monitoring computers, processing software, operators, the rocket, applicable regulations, etc.



The expression of sensitivities

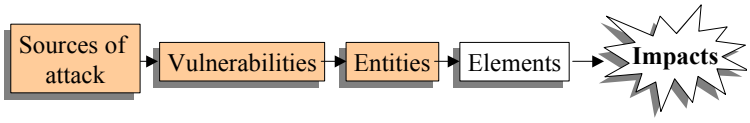
To guarantee that the business operates correctly, the **sensitivity** of each essential element must be expressed.

This expression is based on various **security criteria** such as availability, integrity and confidentiality. If this sensitivity is not covered, there will be an **impact** on the organisation, which may take various forms: financial losses, impaired operation of the activities, loss of customers' confidence, impaired safety for personnel, pollution, etc.

Let us return to the example of the trajectory computation parameter for rocket launching. The availability and integrity requirement for this information should be high to avoid any detrimental impact on personnel safety.

The threat study

Every organisation is exposed to various **threat agents** through its natural environment, culture, image, field of activity, etc.



A threat agent can be characterised by its **type** (natural, human or environmental) and by its **cause** (accidental or deliberate).

It can use various **attack methods** that therefore need to be identified.

An attack method is characterised by the security criteria (availability, integrity, confidentiality, etc.) that it can violate and by the threat agents likely to use it.

Returning to our example, an organisation that launches rockets must take into account a large number of attack methods and threat agents:

- *physical accidents (e.g. fire),*
- *natural events (e.g. seismic phenomenon),*
- *loss of essential services (e.g. loss of electrical power supply),*
- *information compromise (e.g. software entrapment),*
- *technical failures (e.g. equipment dysfunction),*
- *physical attack (e.g. sabotage),*
- *errors (e.g. interpretation error), etc.*

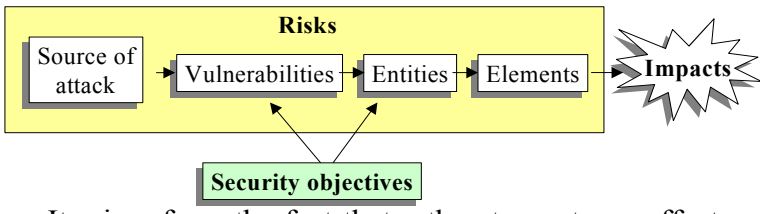
Each entity has **vulnerabilities** that can be exploited by threat agents using each attack method.

We can therefore highlight several vulnerabilities linked to the rocket launching organisation:

- *the possible existence of hidden functions introduced during the design and development phase (software),*
- *use of non-assessed equipment (hardware),*
- *the possibility of creating or modifying system commands (networks),*
- *the network, which can be used to tamper with system resource software (networks),*
- *the ease of intruding into the site through indirect access routes (premises),*
- *operators' failure to comply with instructions (personnel),*
- *the absence of security measures during the design, installation and operation phases (organisation), etc.*

The expression of security objectives

It only remains to determine how the essential elements can be affected by the threat agents and their attack methods: this is the **risk**.



The risk represents possible damage. It arises from the fact that a threat agent can affect the essential elements by using a given attack method to exploit the vulnerabilities of the entities on which they depend.

In our example, there is a risk of sensitive information being compromised by software entrapment arising from the possibility of creating or modifying system commands linked to the network, which could have an impact on personnel safety and customers' confidence.

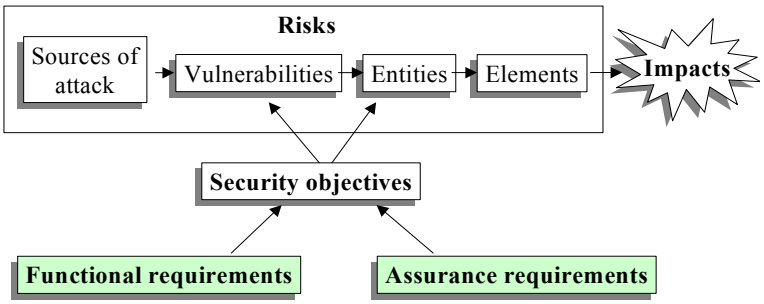
The **security objectives** consist mainly in covering the vulnerabilities of the entities representing all the retained risks.

Clearly, there is no point in protecting what is not exposed. However, as the attack potential increases, the severity of the security objectives must also increase. These objectives therefore constitute a perfectly adapted set of specifications.

One of the security objectives for the rocket launching organisation is to protect the creation and modification of system commands linked to the network.

Determining security requirements

The team in charge of implementing the approach must then produce exact specifications of the required security functionalities. After this, it must demonstrate that the security objectives are perfectly covered by these **functional requirements**.



In our example, one of the functional requirements for protecting the creation and modification of system commands linked to the network is as follows: the system must run a series of selftests at regular intervals during normal operation to demonstrate that it is operating correctly.

Finally, the team in charge must specify the **assurance requirements** allowing the required level of confidence to be obtained and then demonstrated.

One of the assurance requirements is as follows: the developer must carry out a resistance analysis of the system security functions at the required level of resistance.

Summary

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

This straightforward, modular approach can be adapted to all contexts and to various security actions. In addition, EBIOS proves to be an excellent tool for negotiating, decision-making and increasing awareness.

Harmonisation with international standards, its availability as freeware, the training sessions and club for users make EBIOS a resourceful method, maintained at the highest level by experts in the field of information systems security.

For more information:

- the DCSSI Web site http://www.ssi.gouv.fr
- the EBIOS mailbox ebios.dcssi@sgdn.pm.gouv.fr
- the Advisory Office mailbox conseil.dcssi@sgdn.pm.gouv.fr