CLUBEBIOS

EBIOS: the risk management toolbox

Generic approach

Date	:	05/09/2018
Status	:	Approved
Classification	:	Public
Number of pages	:	27
Person responsible for the work	:	Matthieu GRALL
Validation	:	Working group
Approval	:	Board of directors
License	:	

Club EBIOS, 72 avenue Gaston Boissier, 78220 VIROFLAY

Foreword

This document was drawn up by the French information security agency (*Agence nationale de la sécurité des systèmes d'information* – ANSSI) and the Club EBIOS.

ANSSI compiles and updates a wide-ranging methodological reference base designed to help government and private sector bodies to manage the security of their information systems. This reference base is made up of methods, good practise and software, distributed for free on its web site (https://www.ssi.gouv.fr).

The Club EBIOS is an independent non-profit making association (1901 law), made up of individual experts and organizations. It has been bringing together a community of members from the government and private sectors, supporting and contributing to the French risk management reference base since 2003, in collaboration with ANSSI. The Club organizes periodic meetings to facilitate the sharing of experience, the standardization of practises and the satisfaction of users' needs. It also constitutes a forum for defining positions and exercising influence in national and international debates.

Change history

Date	Purpose of the change	Status
02/1997	Version 1 of EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité* / Expression of Needs and Identification of Security Objectives)	Approved
05/02/2004	Version 2 of EBIOS: - Convergence towards ISO/IEC 15408; - Addition of stage 5 – Determining security requirements; - Clarifications and additions, *etc*.	Approved
25/01/2010	Version 3 ("2010") of EBIOS: - Convergence of the concepts with international standards; - Highlighting of stakeholders, communication and cooperation action, monitoring action and review of the descriptions of activities; - Addition of the risk management framework, estimation and assessment of feared events, notions of in-depth defence, residual risks, statement of applicability, action plan and validation; - Study of the threat scenarios by supporting asset and not by vulnerability, *etc*.	Approved
05/09/2018	Version 4 of EBIOS[1]: - Breakdown into a generic approach and specific applications; - Focus on what has not yet been taken into account by the "hygiene" controls and the legal or technical standards; - Risks sources as a departure point for the study; - Taking account of the ecosystem; - Fractal/top-down approach to risks; - Search for efficiency rather than exhaustiveness (or *vice versa*, depending on the context and the objective of the study), *etc*.	Validated

[1] See also "Correspondence with the previous terminology".

Table of contents

1 Introduction

1.1 What is EBIOS?

EBIOS[2] (*Expression des Besoins et Identification des Objectifs de Sécurité* / Expression of Needs and Identification of Security Objectives) allows us to assess and treat risks. It also supplies all the information required for communication within the organization and with its partners, and for validation of the way risks have been treated (see annexe "EBIOS & risk management"). It thus constitutes a complete risk management tool (with respect to the relevant standards, cf. ISO 31000[3]).

This is a real toolbox, from which we choose the actions to be implemented and the method of using them according to the objective of the study. It allows us to assess the risks using scenarios and to develop a coherent policy from them, based on concrete and assessable controls.

1.2 A generic methodology, specific methods

EBIOS, initially designed for information security, can be employed in all fields using the appropriate techniques and knowledge bases.

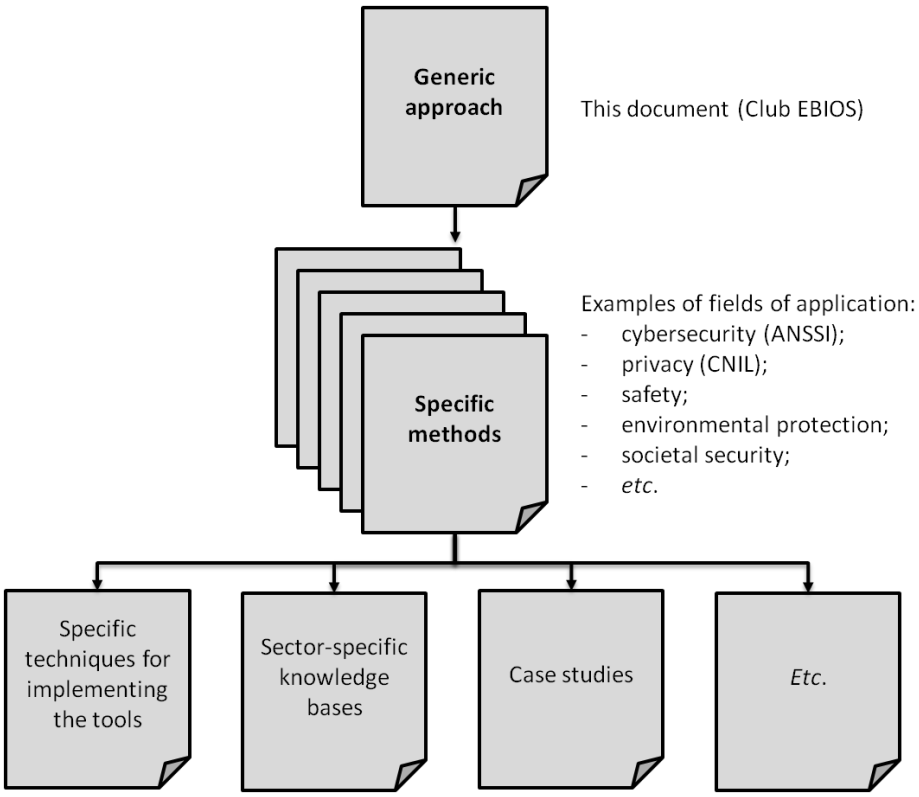

Figure 1 - Breakdown of the generic methodology into specific methods

[2] EBIOS is a trademark registered by the *Secrétariat général de la défense et de la sécurité nationale* (General Defence and National Security Secretariat).

[3] *Risk management – Principles and guidelines for implementation*, International Organization for Standardization – ISO.

EBIOS is flexible enough to be applied to different fields. It has mainly been used to manage information security risks, and also privacy risks, critical infrastructures, the ergonomics of working tools, *etc*. Its convergence, in terms of concepts and strategy, with international standards of management systems and risk management makes it applicable to a large range of fields.

The use of EBIOS in a specific field is relatively easy. It is generally sufficient to adapt the terminology and exploit the techniques and the knowledge bases specific to the field concerned if the knowledge does not seem to be applicable or understood (primary assets, considered criteria, potential impacts, *etc*.). Indeed, each field of application (environmental protection, protection of persons, management of legal risks, *etc*.) has a specific frame of reference, culture and knowledge. But the risk management principles and strategy remain largely the same. Thus, using EBIOS in the framework of the protection of critical infrastructures in the fight against terrorism has involved adapting the vocabulary to the terminology used in this field and creating knowledge bases of criteria, risk sources, supporting assets, specific single actions and integrating government prevention and response plans by way of control bases.

Moreover, different techniques and knowledge bases can be used for each EBIOS module, which makes it easier to integrate EBIOS into the organization's practises.

1.3 Field of application

The risk management strategy described in this guide can be applied:

- To all fields (historically used in the information security field, it has also been used in several other fields);
- To systems currently being developed and to existing systems;
- To the public and private sectors;
- To small structures (small and medium-sized enterprises, regional authorities, *etc*.) large structures (government ministries, international organizations, multinational companies, *etc*.).

1.4 Objectives of the document

The main objectives of this document are:

- To provide a common base of concepts and pragmatic activities for all those involved in risk management, and in particular to create specific methods based on this generic approach;
- To satisfy the risk management needs of all management systems[4];
- To define a comprehensive methodological strategy consistent with and in compliance with internal risk management standards (ISO 31000, ISO 27005[5], *etc*.);
- To establish a reference for the certification of skills related to EBIOS.

[4] Cf. annexe SL of the ISO directives, which defines the common plan and content of all management systems *(ISO/IEC Directives, Part 1 – Consolidated ISO supplement — Procedures specific to ISO*).

[5] *Information technology – Security techniques – Information security risk management*.

2 The main principles

2.1 EBIOS is a toolbox with variable uses

As for all true risk management approaches, EBIOS allows us to identify risks, analyse them, assess them and treat them in the framework of continuous improvement.

EBIOS' special feature resides in its flexibility: this is a real toolbox, in which the activities to be carried out, their level of detail and their sequencing must be adapted to the desired use.

The toolbox is not therefore used in the same way according to the subject considered, the expected deliverables, the recipients and the objective of this communication (decision making, awareness raising, *etc*.) to choose the activities in the strategy to be implemented and to present the results directly in the most appropriate form, but also the degree of knowledge of the scope of the study, the field to which it is to be applied, *etc*.

2.2 Variation of the focal point according to the subject considered

EBIOS allows you to manage the risks relating to subjects of variable size and nature.

EBIOS can be used to manage risks relating to a field of activity, an organization in its entirety, or a sub-division or specific processes of this organization, an information system, a computer system, an interconnection of systems, an application, a security product, a product component, *etc*.

It is obvious that such a wide diversity of subjects cannot be dealt with in a uniform manner if we hope to achieve effective results. It is the level of detail which varies: the broader the subject, the less detail is provided, and *vice versa*. Thus, a highly abstract study may be carried out on macroscopic primary and supporting assets, such as the main activities of an organization and the software as a whole; while a focused study should be carried out on detailed primary and supporting assets, for example the data and a specific version of a database management system.

The toolbox can also be used to study a global subject (e.g. an organization or a complex system made up of several sub-systems), and then to focus on a sub-assembly (e.g. several processes in the organization considered as critical or sub-systems). It is necessary to ensure the consistency of a global study with the studies of its sub-assemblies and between the studies of the different sub-assemblies.

2.3 Variation in depth according to the life span of the study subject

EBIOS allows you to manage risks in all the phases of the life cycle of the study subject; it lends itself in particular to early use in the framework of a development process.

It is recommended to manage the risk right from the initial reflections relating to a new department or a new system. This allows you to decide on the direction of the design and creation, to make choices at an early stage before you have invested too much to be able to go back and start again.

The little knowledge we have of a subject in the initial stage of its life cycle allows us to carry out only a less deep study. The thinking process takes place gradually as you make progress in the work on the subject, by making a series of refinements, according to what you are able to know and to model. At first, we focus on the main challenges so as to identify the "risks relating to the risk sources", subsequently we can refine the description of the subject and develop the "risks at the primary assets' level", then we can study the "risks at the supporting assets' level" to obtain detailed risks and controls, *etc*. It is therefore by performing a series of repetitions and additional activities that risk management guides the subject's life cycle.

Thus, for example, when carrying out studies of the appropriateness and the feasibility of an information system, it is possible to study its context, to identify the main challenges of the system, to develop essential functionalities or processes, to express their needs, estimate the potential impacts and identify the risk sources. A second iteration of the strategy takes place during the general design and the detailed design phase: the main functionalities will be subdivided into more detailed functions and into manipulated information (or other primary assets, according to the field of application), the supporting assets will be identified, the impacts will be refined, the risk sources developed and consolidated, the risk at the supporting assets studied level, the objectives identified, the controls determined and the residual risks highlighted. During the creation phase, another iteration allows us to correct and complement the study, in particular as regards the controls and residual risks. Finally, in the operation phase and up to the end of life of the system, the changes in context (supporting assets, risk sources, risks at the supporting assets' level, *etc*.) allowing the study to be modified and the risks to be managed continuously.

2.4 A general strategy by successive iterations

The risk management strategy is subdivided into five modules:

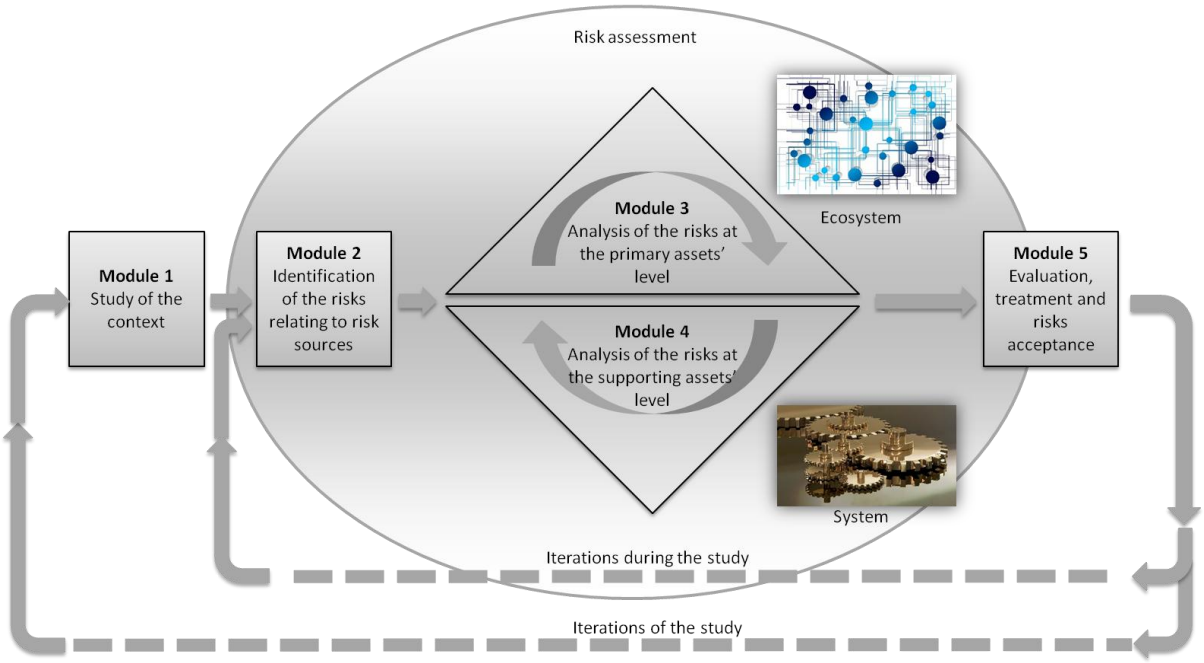

Figure 2 - General approach

EBIOS' approach is iterative: each module will be called upon several times in order to gradually improve the content.

In particular:

- Firstly, Modules 3 and 4 are built by means of successive iterations;
- If the risks are not considered acceptable after Module 5, new iterations must allow us to understand them better and thus to better treat them;
- Finally, the global strategy is refined and updated by means of updating cycles; moreover, it is part of performance assessment and continuous improvement of the whole study.

2.5 Risk assessment by successive refinements

EBIOS' risk assessment takes place in a "fractal" manner in order to understand the high level challenges and their practical foundations:

- First of all, we identify the risks on a macroscopic level ("risks related to risk sources", in Module 2);
- Then, we analyse the risks by refining the scenarios by intermediate and feared events ("risks at the primary assets' level" in Module 3);
- Finally, we the risk analysis is completed by further refining the scenarios by intermediate and feared action ("risks at the supporting assets' level" in Module 4);

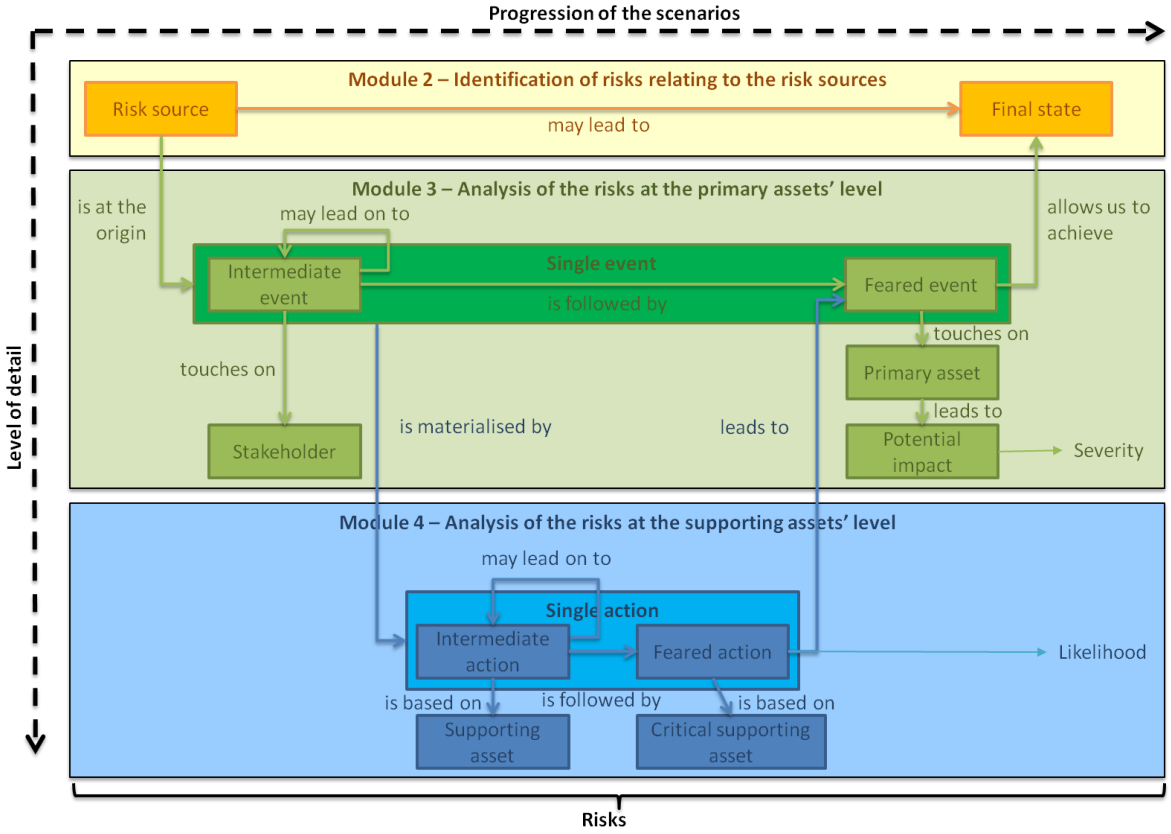

Figure 3 - Risk assessment by successive refinements

Risks refined in this way are then assessed and treated (in Module 5).

Notes: this information is defined in the annexe « Terms and definitions »[6] and used in the following chapters.

[6] See also the annexes "Correspondence with the previous terminology" and "**Erreur ! Source du renvoi introuvable.**".

3 Description of the approach

Module 1 – Study of the context

This module provides the tools to frame the study of risks, identify, delimit and describe the studied object, and its ecosystem.

Tool 1.1. Frame the study of risks

- What is the field of application of the study (cybersecurity, privacy, physical security, environmental protection, societal security, *etc.*)?
- What are the criteria that we want to protect according to the field of application (e.g. availability, integrity and confidentiality for information security)?
- What is the aim of the study (definition or updating of a policy, drafting of specifications, approval, raising awareness of users or of the management, control of the organization's risks, compliance, *etc.*)?
- What are the constraints (technical, organizational, financial, temporal, *etc.*) to be taken into account?
- Who are the actors to be included in the risk management strategy? How?
- How will the information be gathered, cross-referenced, formalized and validated? How is it planned to respond to the questions from the next tools?
- What information can be re-used from previous studies?
- What are the planned validity period of the study and the frequency of revisions?

Tool 1.2. Identify and describe the studied object

- What is the studied object?
- What is the aim of the study? What are the challenges (expected benefits)?
- What are the main functions? Can we make a functional description in diagrammatic form?

Tool 1.3. Identify the reference bases to be complied with

- If applicable, which reference bases are to be complied with (legal or technical standards, sector-specific reference bases, internal policies, *etc.*)?
- What is their implementation status? Have deviations been identified? Have they been the subject of arbitration?

Tool 1.4. Identify the components of the ecosystem

- Which stakeholders is the studied object interacting with? What are their links (between themselves and with the studied object, e.g. organizational, technical, functional, contractual, *etc.*)?
- If possible, what are their characteristics (dependence, maturity, *etc.*)?
- Which characteristics shall we select in the rest of the study (according to their relevance, if we want to deal with the essential points as quickly as possible)?

Module 2 – Identification of risks relating to the risk sources

This module provides the tools to identify and characterize the risks at a macroscopic level, in the form of couples {source of risk in the ecosystem/final state that it may lead to for the studied object or for the ecosystem}. These couples {risk source / final state} thus identified constitute high level risk scenarios, which will be assessed in modules 3 and 4 by successive refinements.

Tool 2.1. Identify the risk sources that are relevant for the studied object

- What are the risk sources that are relevant for the studied object?
- How can we characterize them (internal or external, human, natural or other; of accidental or intentional origin; *etc*.)?
- Which risk sources shall we use in the rest of the study (according to their relevance, if we want to deal with the essential points as quickly as possible)?

Tool 2.2. Determine the final states that they may lead to

- What final states might they lead to (or search for, in the case of risk sources acting deliberately) on the studied object or on the ecosystem?
- Which final states shall we use in the rest of the study (according to their relevance, if we want to deal with the essential points as quickly as possible)?

Tool 2.3. Assess the relevance of the risks relating to risk sources

- If possible, what are the capacities of the risk sources to generate each final state (according to their resources, their expertise, their dangerousness, their professional or personal context for human sources, their motivations for those acting deliberately, *etc*.)?
- If possible, what are the procedures (actions necessary to obtain a result) usually associated with these risk sources for these final states?
- What risks relating to the risk sources (couples {risk source/final state}) shall we use in the rest of the study (according to their relevance, if we want to deal with the essential points as quickly as possible)?

Module 3 – Analysis of the risks at the primary assets' level

This module provides the tools to start to analyse the risks selected in Module 2. The analysis is carried out at the level of the primary assets and not of their supporting assets. It consists in studying the "functional" scenarios of the risk sources. They may include a succession of intermediate events on different stakeholders and feared events on the primary assets, or at least one feared event on one primary asset. The risks analysed in this way are assessed in terms of severity.

Tool 3.1. Identify the primary assets

- What are the primary assets (according to the field of application of the study and the desired level of detail, e.g. functions, information, persons, assets, *etc*.)?
- Which assets shall we select in the rest of the study (according to their relevance, if we want to deal with the essential points as quickly as possible)?

Tool 3.2. Analyse the "functional" scenario of risk sources

- If the risk sources were to pass through the stakeholders, which ones would they pass through to lead to each final state and in which sequence?
- What could they do to each stakeholder (intermediate events)?
- What could they do to the primary assets (feared events and criteria affected)?
- What are the potential impacts of each feared event made up in this way (several types of impact may be considered)?

Tool 3.4. Assess the severity of each risk at the primary assets' level

- What is the relevant scale in the context of the study in order to assess the severity (a global scale or a scale for each type of impact, e.g. Negligible, significant, important or maximum)?
- What are the existing or planned controls contributing to reducing the severity of each risk at the primary assets' level?
- What level of the severity scale does each risk correspond to, in particular according to the potential impacts, and also the risk sources (motivations, potential for harm, *etc*.) and the existing or planned controls?
- If possible, how can we justify each estimation (illustrations, examples of potential impacts, volumes concerned, existing or planned controls, *etc*.)?

Module 4 – Analysis of the risks at the supporting assets' level

This module provides the tools to carry out an in-depth analysis of the risks selected in Module 3. The analysis is carried out on the supporting assets and not on the primary assets. It consists in studying the "practical" scenarios of the risk sources. They may include a succession of intermediate actions on different supporting assets and feared actions on critical supporting assets, or at least one feared action on one critical supporting asset. The risks analysed in this way are assessed in terms of likelihood.

Tool 4.1. Identify the supporting assets

- What are the supporting assets on which the primary assets rely?
- What are those that we consider to be critical? Why?
- Which supporting assets shall we use in the rest of the study (according to their relevance, if we want to deal with the essential points as quickly as possible)?

Tool 4.2. Analyse the "practical" scenario of risk sources

- Which supporting assets would they pass through to generate each feared event and in what sequence?
- What could they do to each supporting asset (intermediate events)?
- What could they do to the critical supporting assets (intermediate events)?
- What are the vulnerabilities of the supporting assets, exploitable in the framework of each feared action thus constituted?

Tool 4.4. Assess the likelihood of each risk at the supporting assets' level

- What is the relevant scale in the context of the study to assess the likelihood (e.g. negligible, significant, important or maximum)?
- What are the existing or planned controls contributing to reducing the likelihood of each risk occurring for the supporting assets?
- What level of the likelihood does each risk correspond to, in particular with respect to the vulnerabilities of the supporting assets, but also the risk sources (proximity of the studied object, effort necessary, motivations, capacities, feeling of impunity, response expected, *etc*.) and the existing or planned controls?
- If possible, how can we justify each assessment (illustrations, incidents that have occurred, existing or planned controls, *etc*.)?

Module 5 – Evaluation, treatment and risks acceptance

This module provides tools for assessing the risks that have been identified in Module 2 and analysed successively in Modules 3 and, for determining the means to treat them and deciding to accept the residual risks or not.

Tool 5.1. Evaluating the risks

- What is the right level of detail to present the risks at (per risk related to the risk sources, per risk at the primary assets' level, per risk at the supporting assets' level, per feared event, *etc.*) according to the study context and the persons for whom it is intended?
- What are the risks according to the level of detail chosen? (e.g. risks at the primary assets' level, with for each one a list of risks at the supporting assets' level which allows its occurrence, their severity being equal to that of the risk at the primary assets' level, and their likelihood being equal to the maximum likelihood of the risks at the supporting assets' level)
- If possible, how can we represent them visually? (e.g. by positioning each risk on a diagram with its likelihood on the X-axis and the severity on the Y-axis, or on a radar with the highest risks near to the centre) How can we illustrate each risk by an explicit example?
- What is the relevant scale in the context of the study to assess the risks? (e.g. negligible, significant, important or maximum)
- What level of the evaluation scale does each risk correspond to with respect to its severity and its likelihood?

Tool 5.2. Identify the objectives

- What is the relevant form of the objectives (tactics to be prioritised for dealing with each risk[7] and/or general objectives for the ecosystem and/or state desired for each support after the risks have been treated, *etc.*) according to the study context and the persons for whom it is intended?
- What are the objectives that we identify with respect to the risks? Can these objectives be laid down in a contract with those who will have to satisfy them?

Tool 5.3. Demonstrate the satisfaction of the reference bases to be complied with

- Where relevant, have the requirements of each reference base to be complied with been met (e.g. explain how they met the requirements or justify why they do not meet them)?

[7] Several tactics can be envisaged:

- By types of controls to be prioritized (prevention, protection, recovery, *etc.*);
- By component of the risks to be dealt with as a priority (risk sources, supporting assets, primary assets, risks for the supporting assets, potential impacts, *etc.*);
- By risk processing option (reduce it, share it, refuse it, maintain it), *etc.*

Tool 5.4. Determine the additional controls to be implemented

- For each objective identified, what are the additional controls (in addition to the reference bases to be complied with and to the existing or planned controls, where relevant) that should be implemented to achieve it?
- For each control determined, what is the concrete plan of action to implement it (person responsible, difficulty, financial cost, time limit, *etc*.)?

Tool 5.5. Accept the residual risks

- What are the residual risks (re-assess the severity and the likelihood of each risk occurring, taking account of the additional controls determined)?
- Are the residual risks and the way it is planned to deal with the risks considered to be acceptable? If not, repeat the previous steps!

Tool 5.6. Monitoring risks and continuous improvement

- What are the relevant indicators for measuring the changes in and/or the occurrence of each residual risk?
- Has each control been implemented? What is its real efficiency?
- How do we manage the experience feedback and continuous improvement process?
- Are the updating cycles defined at the beginning of the studies appropriate?

Annexes

Terms and definitions

Control *(Mesure)*	Means of treating with a risk. *Note(s): a control may take various forms according to the context and the study objective.* *For example:* - *All the controls which make up a policy;* - *A control may be technical or organizational;* - *Some controls may be mutually reinforcing and act according to complementary axes or dimensions (notion of in-depth defence);* - *It is part of an option for dealing with the risk (reduction, sharing, refusal, maintenance) which has been the subject of a decision;* - *A control is generally carried by a supporting asset;* - *A control may act on a risk source, a supporting asset, a primary asset or a potential impact.*
Criterion *(Critère)*	Property to be guaranteed. *Example(s): confidentiality, integrity, availability.* *Note(s):* - *The criterion applies to a primary asset;* - *It is affected by an action on a support.*
Critical supporting asset *(Support critique)*	Supporting asset considered by the organization as having a critical character for the primary asset(s) that it supports. *Note(s): the compromizing of a critical supporting asset necessarily leads to an attack on the primary assets that it carries.*
Ecosystem *(Écosystème)*	Whole made up of the stakeholders interacting with the studied object. *Note(s):* - *By "interaction" we mean all relationship which arising in the normal operation of the studied object;* - *The risk sources are not necessarily considered as stakeholders, except if they are legitimately interacting with the studied object elsewhere.*
Feared action *(Action redoutée)*	Single action affecting a critical supporting asset. *Note(s):* - *Constituting the technical foundation of a feared event, it*

	describes the organization's point of view regarding a risk at the supporting assets' level; - *It represents the action of a risk source on a critical support and the criteria affected on the associated primary asset;* - *It is assessed in terms of likelihood.*
Feared event *(Événement redouté)*	Single event on a primary asset. *Note(s):* - *It describes the organization's point of view regarding a risk at the primary assets' level;* - *it represents the action of a risk source on a criteria of a primary asset and its potential impacts;* - *It is estimated in terms of severity.*
Final state *(État final)*	Last situation of the studied object and/or of the ecosystem, resulting from actions of a risk source. *Example(s): commercial data stolen and resold, main activity of the company interrupted, market share lost, climate of fear reached, loss occurred, etc.* *Note(s): it may constitute an aim (in the case of a risk source acting deliberately) or it is unforeseeable (in the case of a risk source acting accidentally manner).*
Intermediate action *(Action intermédiaire)*	Single action affecting a supporting asset.
Intermediate event *(Événement intermédiaire)*	Single event on a stakeholder.
Likelihood *(Vraisemblance)*	Assessment of the possibility of occurrence of a risk. *Example(s): negligible, limited, important, maximum.* *Note(s): the likelihood of a risk is generally the maximum likelihood of the risks at the supporting assets' level concerned.*
Objective *(Objectif)*	Direction decided upon to treat a risk. *Note(s): this direction may be expressed either by a chosen treatment option (reduction, sharing, refusal, maintenance) or by an expected residual risk level.*
Potential impact	Potential consequence of a risk for the studied object and/or its

(Impact potentiel)	ecosystem. *Note(s):* - *The impact may be direct or indirect;* - *It may relate to the brand image, financial losses, invasion of privacy, etc.*
Primary asset *(Élément à protéger)*	Asset which is essential in the framework of the studied object according to its field of application. *Example(s): information (e.g.: invoices, personal information, prices, etc.), processes (e.g.: placing an order, managing stock, etc.), personal data (e.g.: login, e-mail address, IP address, etc.), persons (e.g.: employees, visitors, etc.), places (e.g.: site, housing, waterway, etc.).*
Risk *(Risque)*	Scenario from end to end, describing a risk at the primary assets' level and all the risks at the supporting assets' level which may create it. *Note(s):* - *It is initiated by a risk source and tends to lead to a final state;* - *It is assessed in terms of severity and likelihood of occurrence.*
Risk at the primary assets' level *(Risque au niveau des éléments à protéger)*	Procedure describing the sequence of single events and of the feared event caused by a risk source in the ecosystem and likely to lead to a final state. *Note(s):* - *It describes a "functional" scenario;* - *It is made up of a risk source, possible single event for stakeholders, a feared event for a primary asset, and a final state;* - *It is assessed in terms of severity.* - *A risk at the primary assets' level will only be selected if it really contributes to the achievement of a final state, i.e. if it includes at least one feared event contributing to the final state.*
Risk at the supporting assets' level *(Risque au niveau des supports)*	Procedure describing the sequence of single actions and feared action carried out by a risk source in order to create a risk at the primary assets' level. *Note(s):* - *It describes a "practical" scenario;* - *It is made up of risk source, possible single actions on supporting assets and a feared action for a critical supporting asset;* - *It is assessed in terms of likelihood;* - *A risk at the supporting assets' level may produce effects corresponding to a risk at the primary assets' level not initially targeted (the notion of collateral effects);*

- *A risk at the supporting assets' level will only be selected if it really contributes to the creation of a risk at the primary assets' level, i.e. if it includes at least one feared action, contributing to the feared event of the risk for a primary asset.*

Risk source

(Source de risque)

A thing or a person, group of persons or organization, at the origin of one or several risk(s).

Example(s): governmental department, hacker, competitor, employee, animal, water, fire, the passing of time.

Note(s): in the case where controls have already been put in place to counter accidental risks, e.g. by means of a security study or reliability study, it is possible to limit ourselves to intentional risk sources.

Severity

(Gravité)

Assessment of the extent of the effects of a risk.

Example(s): negligible, limited, important, maximum.

Note(s): the severity of a risk is generally the severity of the risk at the level of the primary assets concerned.

Single action

(Action élémentaire)

An elementary action performed by a risk source in the framework of a risk at the supporting assets' level.

Example(s): exploit a software vulnerability, copy files, delete evidence.

Single event

(Événement élémentaire)

A single event caused by a risk source in the framework of a risk at the primary assets' level.

Note(s):

- *It results in practise from the occurrence of a risk at the supporting assets' level by a risk source.*

Stakeholder

(Partie prenante)

System, person or organization which may affect or be affected by a decision or an activity in the framework of the studied object.

Example(s): organization, service provider, client.

Studied object

(Objet de l'étude)

Studied organization or system.

Supporting asset

(Support)

Asset in the information system on which one or several primary assets rely.

Example(s): technical sub-system, server, trade software, network, system administrator.

Note(s):

- *It may be a sub-system or more specifically hardware, software, network, person, etc.;*

- *The supporting asset is the practical target of the risk source;*
- *A target supporting asset must be observed not only with respect to the (possible) attack on the primary asset that it carries, but also with respect to its possible exploitation by the risk source in a risk at the supporting assets' level.*

Correspondence with the previous terminology

New terms	Previous terms	Equivalent terms in ISO 31000
Single action	-	-
Intermediate action	Threat	-
Feared action	-	-
Criterion	Security criterion	-
Ecosystem	External context	-
Primary asset	[identical]	-
Final state	-	-
Single event	-	-
Intermediate event	-	-
Feared event	[identical]	-
Severity	[identical]	-
Potential impact	Impact	Consequence
Control	Security control	-
Objective	Security objective	-
Stakeholder	[identical]	-
Risk	[identical]	Risk
Risk at the primary assets' level	-	-
Risk at the supporting assets' level	Threat scenario	Event
Risk source	Threat source	Risk source
Supporting asset	[identical]	-
Critical supporting asset	-	-
Likelihood	[identical]	Likelihood

EBIOS & risk management

The challenge: achieve its objectives on the basis of rational decisions

Originating in the financial field in the 1950's and then extended to a number of other fields such as project management, security of persons, safety, marketing, the environment, information security and privacy, risk management has always aimed to rationalize situations to help make informed decisions. The choices made by the deciders can thus be made with respect to elements provided by *risk managers*. And these choices can guide the organization towards achieving its objectives and can also develop its strategy.

Different practises but common principles

At the present time, the common principles of risk management can be found in international standards (in particular ISO 3000):

- Risk is defined as the effect of uncertainty on the achievement of objectives. It is characterized by an event, its consequences and its likelihood;
- The process of risk management includes the establishment of the context, risk assessment, risk treatment (including the validation of risk treatment), communication and consultation relating to the risks, monitoring and review (control), and the recording and drawing up of reports, in a continuous improvement cycle.

The similarity of the concepts and methods of analysis shows that there is a risk management model that is sufficiently generic to be shared and improved by multidisciplinary experience feedback:

- The risks can be described according to their cause and their direct and indirect impacts for the security of persons;
- By the circumstances that are at the origin of the risk and their consequences for the legal risks;
- In terms of scenarios describing how the risk sources will be able to exploit the vulnerabilities of the systems to achieve their objective and affect the security of primary assets and the organization, as is the case in cybersecurity;
- By scenarios describing the actions of risk sources on systems processing personal data and their potential impacts on the rights and freedoms of persons in the field of privacy;
- Without forgetting the term specific to the protection of critical infrastructures or to the practises of economic intelligence.

Risk management must therefore allow the creation of value, be integrated into organizational processes, be integrated into decision-making, explicitly handle uncertainty, be systematic, structured and used in a timely manner, be based on the best available information, be tailor made, integrate human and cultural factors, be transparent and participative, be dynamic, iterative and responsive to change, and facilitate improvement and the continuous evolution of the organization.

EBIOS incorporates all these dimensions.

How does EBIOS allow you to manage risk?

Establishing the context

A well-defined context allows you to manage risks in a completely appropriate manner, and thus reduce the costs to what is necessary and sufficient with respect to the reality of the studied subject. To do so, it is essential to understand the elements to be taken into account:

- The framework put in place to manage risks;
- The estimation, evaluation and risk treatment validation methods;
- The description of the scope of the study and its environment (external and internal context, constraints, listing of assets and their interactions, *etc*.).

EBIOS' toolbox allows us to consider all these points according to the degree of knowledge we have of the studied subject. It will then be possible to develop, refine and improve as our knowledge of the subject improves.

Risks assessment

There is a risk whenever there is uncertainty about an event which has consequences for the objectives. In particular, this can become reality whenever there is an event and consequences simultaneously. We can therefore understand that there is no longer a risk if one of these factors is lacking (feared event or consequence). However, it is extremely difficult, and even dangerous, to affirm with certainty that one of the factors is absent. Also, each of the factors may contribute to a number of different risks, which can themselves link up or combine into more complex scenarios, which are nevertheless just as realistic.

We will therefore study each of these factors, in the broadest manner possible. We can then highlight the important factors, understand how they can combine, estimate and assess (organize into a hierarchy) risks. An important challenge is to succeed in obtaining the necessary information which can be considered as reliable. This is why it is extremely important to ensure that this information is obtained in such a way that it limits bias and that the method is reproducible.

To do this, the EBIOS toolbox focuses first of all on primary assets (risk sources, criteria and impacts generated in the event of failure to meet these criteria), then on their supporting assets (risk sources, actions and vulnerabilities). The risks may then be identified by combining the feared events and the procedures, then estimated and assessed in order to obtain a hierarchical list according to their importance.

Risks treatment

The assessed risks allow you to take objective decisions in order to maintain them at an acceptable level, taking account of the specificities of the context.

To do so, EBIOS allows you to choose the treatment of the assessed risks by means of objectives: it is thus possible, for all or part of each risk, to reduce it, to share it (entrust part of the risk to a third party who is better equipped to deal with it), to refuse it (put yourself in a situation where the risk does not exist) or maintain it (implement no additional controls). Controls can then be proposed and negotiated in order to achieve these objectives.

The manner in which the risks have been managed, and the residual risks which remain after treatment, must be validated, if possible formally, by an authority responsible for the scope of the study. This validation is carried out on the basis of a file whose contents are the result of the study carried out.

Communication and consultation relating to the risks

Obtaining relevant information, presenting the results, having decisions taken, validating the choices made, raising awareness of the risks and security control to be applied correspond to communication activities which are carried out before, during and after the study of the risks.

This communication and consultation process relating to the risks is a crucial factor in the success of risk management. If this is carried out effectively, and in a manner appropriate to the culture of the organization, it contributes to the involvement, accountability and awareness of the actors. It creates a synergy around information security, which contributes significantly to developing a real security and risk culture within the organization.

The involvement of the actors in the process of risk management is necessary to define the context in an appropriate manner, ensure an in-depth understanding of the interests of the actors and also ensures that these interests are taken into account, to group different fields of expertise together to identify and analyse the risks, to ensure that the different points of view are taken into account in the risk assessment, to facilitate the appropriate identification of risks, the application and secure implementation of a treatment plan.

Monitoring and reviewing risks

The framework put in place for managing risks, and the results obtained, must be relevant and kept up to date in order to take account of the changes in the context and the improvement previously identified. This continuous improvement strategy must be based on performance indicators and, where applicable, allow its integration into a contractual framework.

Recording and drawing up reports

The strategy and the tools chosen must be formalised. They may be drawn up in documents that may be distributed or not, depending on whether there is a desire to build trust through transparency, and also the need to protect industrial secrets and the security of the organization.

Coverage of the standard ISO 31000

The following diagram shows the correspondence between EBIOS tools and the ISO 31000 standard:

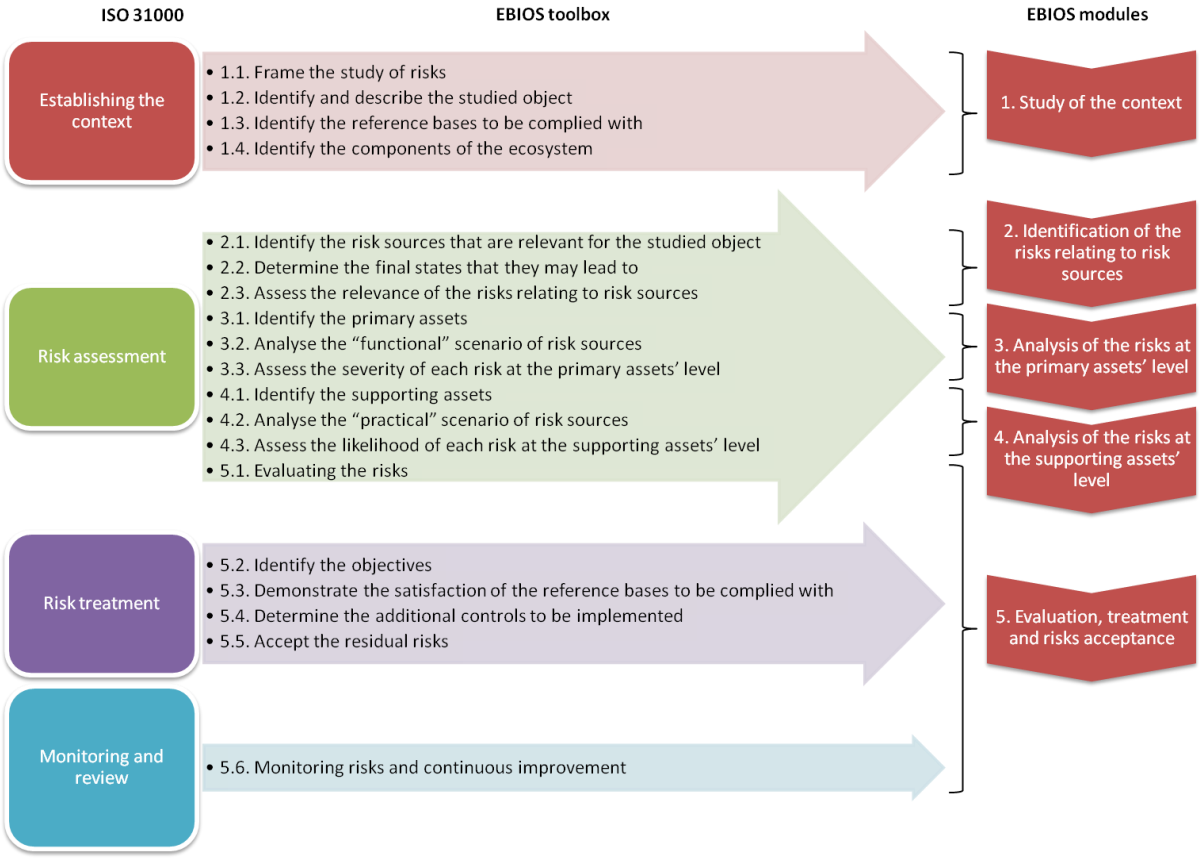

Figure 4 - Correspondence between EBIOS tools and ISO 31000