

EBIOS

RISK MANAGER



CONTENTS

WHAT IS THE EBIOS RISK MANAGER METHOD?	<i>page 2</i>
AN ITERATIVE APPROACH IN 5 WORKSHOPS	<i>page 3</i>
DIFFERENT USES OF EBIOS RISK MANAGER	<i>page 13</i>
	
WORKSHOP 1 – SCOPE AND SECURITY BASELINE	<i>page 15</i>
WORKSHOP 2 – RISK ORIGINS	<i>page 31</i>
WORKSHOP 3 – STRATEGIC SCENARIOS	<i>page 39</i>
WORKSHOP 4 – OPERATIONAL SCENARIOS	<i>page 55</i>
WORKSHOP 5 – RISK TREATMENT	<i>page 67</i>
	
BIBLIOGRAPHY	<i>page 79</i>
TERMS AND DEFINITIONS	<i>page 81</i>

WHAT IS THE EBIOS RISK MANAGER METHOD?

EBIOS Risk Manager¹ (EBIOS RM) is the method for assessing and treating digital risks published by National Cybersecurity Agency of France (ANSSI) with the support of Club EBIOS². It proposes a toolbox that can be adapted, of which the use varies according to the objective of the project, and is compatible with the reference standards in effect, in terms of risk management³ as well as in terms of cybersecurity⁴.

EBIOS RM makes it possible to assess digital risks and to identify the security measures to be taken in order to control them. It also makes it possible to validate the acceptable level of risk and to carry on in the longer term in a continuous improvement approach. Finally, this method makes it possible to bring about resources and arguments that are useful for communication and decision-making within the organisation and with regards to its partners.

The EBIOS RM method can be used for several purposes:

- setting up or reinforcing a management process of the digital risk within an organisation;
- assess and treat the risks relating to a digital project, in particular with the aim of a security accreditation;
- define the level of security to be achieved for a product or service according to its use cases and the risks to be countered, in the perspective of a certification or accreditation for example.

It applies to public as well as private organisations, regardless of their size, their sector of activity and whether their information systems are being developed or already exist.

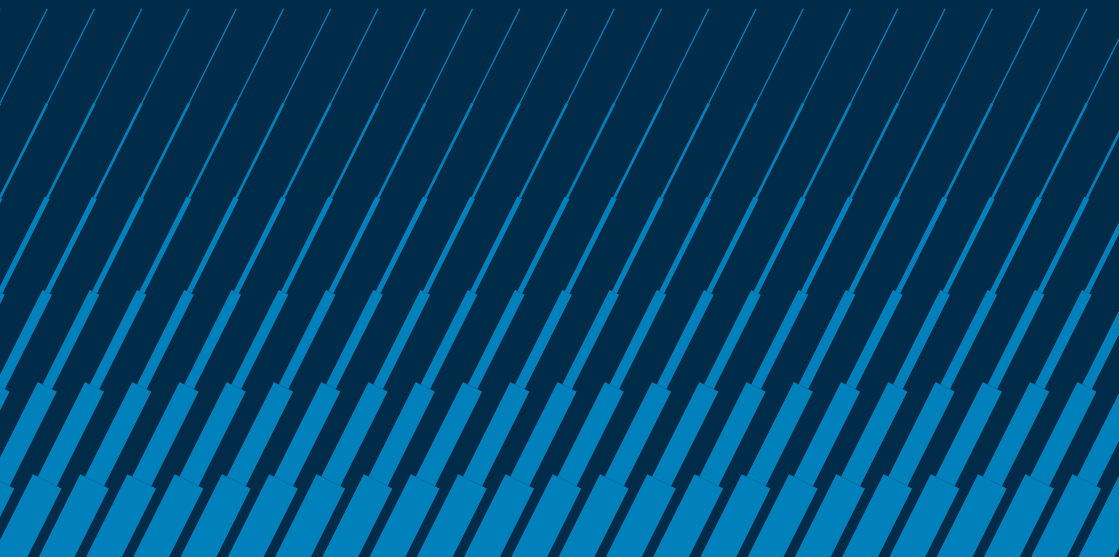
1 EBIOS is a registered trademark of the Secrétariat général de la défense et de la sécurité nationale (General Secretariat for Defence and National Security).

2 Club EBIOS is an association governed by the law of 1901 bringing together individual experts and bodies, coming from public or private sectors. It has been supporting and enriching the French reference standards for managing risks since 2003.

3 In particular, standard ISO 31000:2018

4 In particular the standards in the series ISO/IEC 27000.

**An iterative
approach in 5
workshops**



The EBIOS Risk Manager method adopts an approach to the management of the digital risk starting from the highest level (major missions of the studied object) to progressively reach the business and technical functions, by studying possible risk scenarios. It aims to obtain a synthesis between "compliance" and "scenarios", by positioning these two complementary approaches where they provide the highest value added. This approach is symbolised by the digital risk management pyramid (cf. figure 1).

The approach through compliance is used to determine the security baseline on which the approach through scenarios is based in order to develop particularly targeted or sophisticated risk scenarios. This assumes that the accidental and environmental risks are treated *a priori* via an approach through compliance within the security baseline. The assessment of the risks through scenarios, such as described by the EBIOS RM method, therefore focuses on the intentional threats.

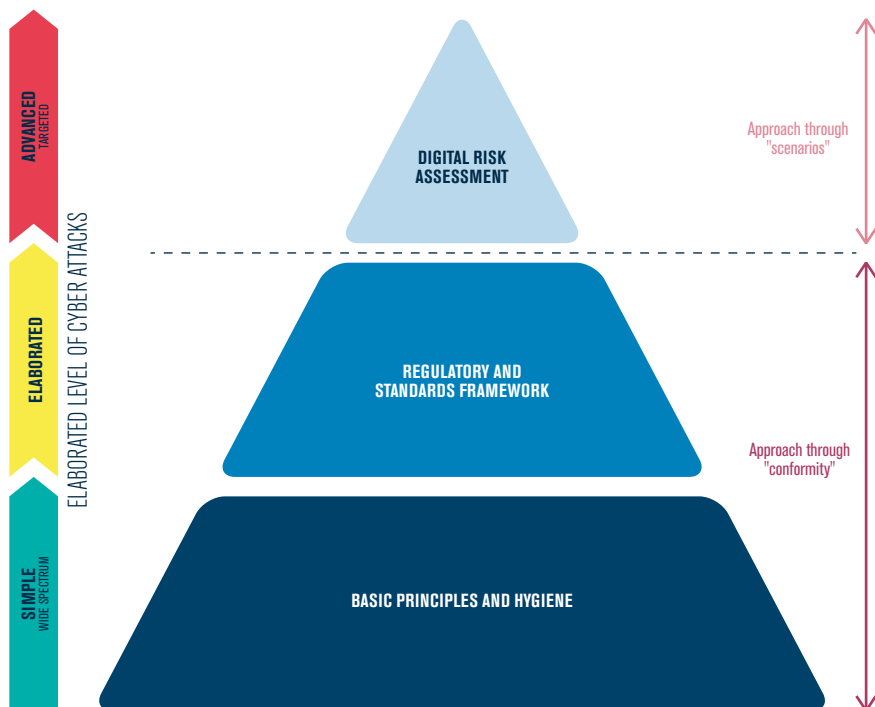
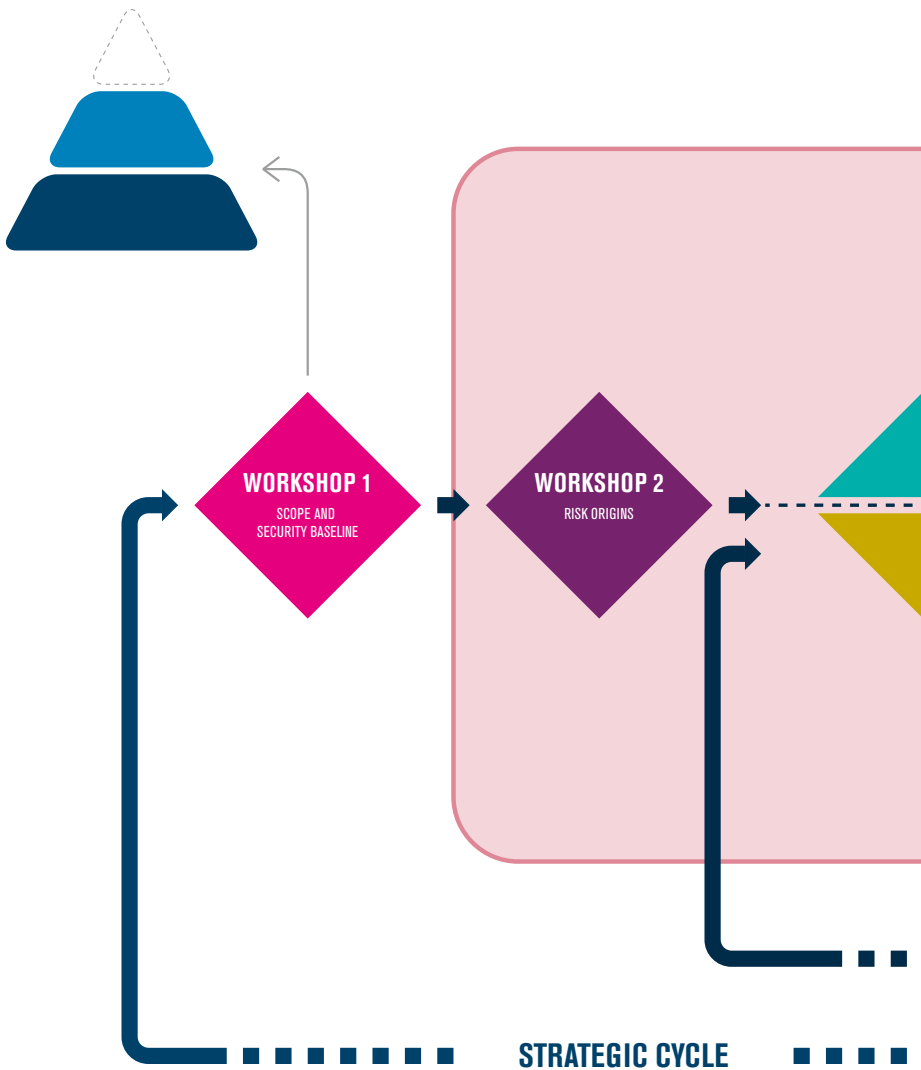
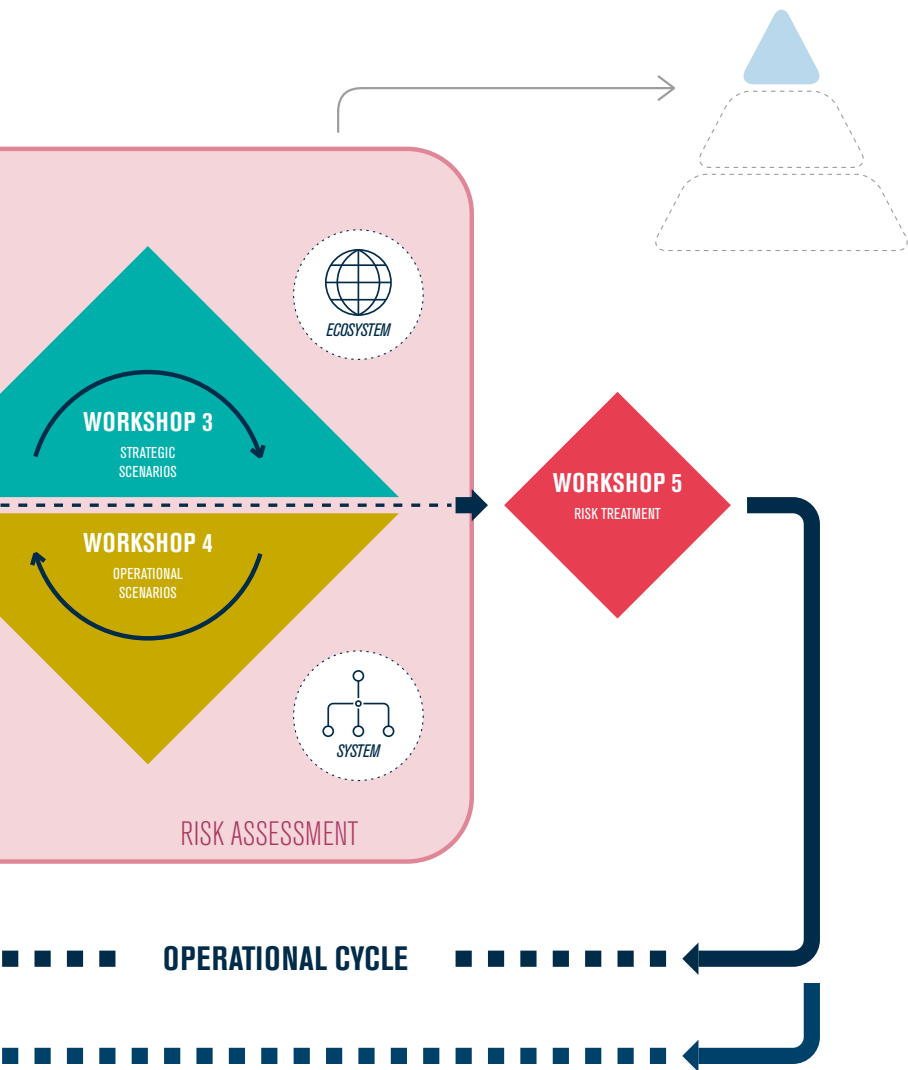


Figure 1 — Digital risk management pyramid

THE EBIOS RM METHOD ADOPTS AN ITERATIVE APPROACH THAT REVOLVES AROUND FIVE WORKSHOPS.

Figure 2 — An iterative approach in 5 workshops





WORKSHOP 1

Scope and security baseline

The first workshop aims to identify the studied object, the participants in the workshops and the timeframe. During this workshop, you will list the missions, business assets⁵ and supporting assets related to the studied object. You identify the feared events associated with the business assets and assess the severity of their impacts. You also define the security baseline and the differential.

NOTE: workshop 1 makes it possible to follow an approach by "compliance", corresponding to the first two stages of the digital risk management pyramid and to address the study from the "defence" viewpoint.



WORKSHOP 2

Risk origins

In the second workshop, you identify and characterise the risk origins (RO) and their high-level targets, called target objectives (TO). The RO/TO pairs deemed the most relevant are selected at the end of this workshop. The results are formalised in a mapping of the risk origins.

5 The "business assets" correspond to the "essential assets" of the EBIOS 2010 method.

WORKSHOP 3

Strategic scenarios

In workshop 3, you will get a clear view of the ecosystem and establish a mapping of the digital threat of the latter with respect to the studied object. This will allow you to construct high-level scenarios, called strategic scenarios. They represent the attack paths that a risk origin is likely to take to reach its target. These scenarios are designed at the scale of the ecosystem and the business assets of the studied object. They are assessed in terms of severity. At the end of this workshop, you can already define the security measures on the ecosystem.



WORKSHOP 4

Operational scenarios

The purpose of workshop 4 is to construct technical scenarios that include the methods of attack that are likely to be used by the risk origins to carry out the strategic scenarios. This workshop adopts an approach similar to the one of the preceding workshop but focuses on critical supporting assets. You then assess the level of likelihood of the operational scenarios obtained.

NOTES

- Workshops 3 and 4 are naturally supplied during successive iterations.
- Workshops 2, 3 and 4 make it possible to assess the risks, which constitutes the last stage of the digital risk management pyramid. They use the security baseline according to different attack paths, which are relevant with regards to the threats considered and as a limited number in order to facilitate the analysis.

WORKSHOP 5

Risk treatment

The last workshop consists in creating a summary of all of the risks studied in order to define a risk treatment strategy. The latter is then broken down into security measures written into a continuous improvement plan. During this workshop, you establish the summary of the residual risks and define the framework for monitoring risks.

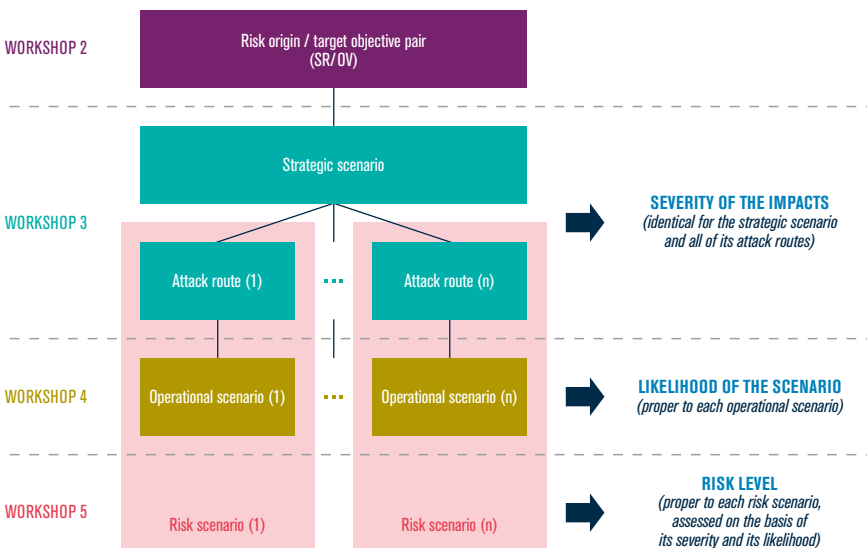


Figure 3 — Link between the various workshops

NOTE : each attack path of a strategic scenario gives rise to an operational scenario. A risk scenario corresponds to the association of an attack path and its operational scenario.

THE CYCLES

The approach calls for two cycles, of which the durations are defined during the first workshop:

- a strategic cycle that revisits the entire study and in particular the strategic scenarios;
- an operational cycle that returns to the operational scenarios in light of the security incidents that have occurred, the appearance of new vulnerabilities and changes in the methods of attack.



AN EXAMPLE FOLLOWED STEP-BY-STEP

The method is illustrated using an example that depicts a fictive company, namely a biotechnology company that manufactures vaccines. This example aims to be realistic with the objective of providing the reader with a concrete and pedagogical illustration of the method.



BIOTECHNOLOGY COMPANY MANUFACTURING VACCINES



Estimation of a low level of maturity in terms of digital security



Basic awareness in cybersecurity when employees take up their jobs



Existence of an IT charter

Different uses of EBIOS Risk Manager

EBIOS RM is a method that can be adapted. It constitutes a genuine toolbox, of which the activities to be carried out, their level of detail and their sequencing, will be adapted to the desired use. Indeed, the way in which the method is applied differs according to the subject studied, the expected deliverables, the degree of knowledge of the perimeter of the study or the sector to which it is applied. The chart hereinafter suggests use cases according to the target objective.

TARGET OF THE STUDY	MAIN WORKSHOPS TO BE CONDUCTED OR USED				
	1	2	3	4	5
Identify the security baseline adapted to the studied object	X				
Be in compliance with the digital security reference standards	X				X
Assess the threat level of the ecosystem with respect to the object studied			X <i>(note 1)</i>		
Identify and analyse the high-level scenarios, integrating the ecosystem		X	X		
Conduct a preliminary risk study in order to identify the priority axes for security improvement	X <i>(note 2)</i>	X	X		X <i>(note 3)</i>
Conduct a complete and fine risk study, for example on a security product or for the purpose of a system accreditation	X	X	X	X	X
Direct a security audit and in particular a penetration test			X	X	
Direct the detection and reaction systems, for example at the level of a security operating centre (SOC)			X	X	

NOTE 1: step a) of the workshop only; this does not require having conducted workshops 1 and 2 beforehand.

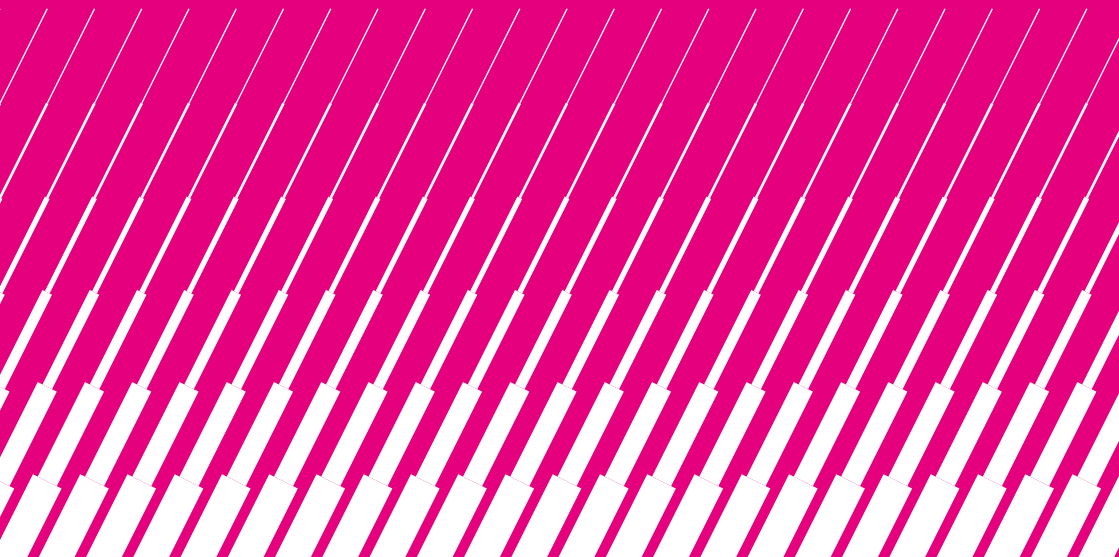
NOTE 2: in the framework of a preliminary study, the degree of depth of workshop 1 is to be adapted (example: listing only the business assets, conducting a summary analysis of the security baseline).

NOTE 3: step b) of the workshop only.

WORKSHOP



**Scope and
security baseline**



1/ Objectives of the workshop

The purpose of this first workshop is to define the framework of the study, its business and technical scope, the associated feared events and the security baseline. This workshop is a prerequisite for producing a risk assessment. The period to be considered for this workshop is the same as the strategic cycle.



2/ Participants in the workshop⁶

- Top management;
- Business teams;
- CISO (Chief Information Security Officer);
- IT department / Information management team.



3/ Outputs

At the end of this workshop, you must have identified:

- the framework elements: objectives, roles and responsibilities, time frame;
- the business and technical scope : missions, business assets, supporting assets;
- feared events and their level of severity;
- the security baseline: list of applicable requirements, implementation status, gaps identification and justification.

⁶ The team can be supplemented with any person deemed helpful.

4/ Steps of the workshop

This workshop can for example take place over one to three half-day sessions⁷. The objective will be to:

- a. define the framework of the study;
- b. define the business and technical perimeter of the studied object;
- c. identify the feared events and assess their level of severity;
- d. determine the security baseline.



5/ How to proceed?

a DEFINE THE FRAMEWORK OF THE STUDY

To initiate the workshop, start with disclosing the purpose and the expectations of the meeting to the participants. Agree on the **objectives** of the study. The latter can be, for example, the setting up of a cyber risk management process in the organisation, the accreditation of an information system or the identification of a level of security to be achieved in order to obtain a product certification. According to the objective defined, the level of detail of the study is deduced therefrom, along with the workshops to be conducted.

Then, identify the **participants** in the various workshops, their roles and their responsibilities in the framework of the study (workshop facilitator, contributor, decision-maker, etc.). To do so, you can for example create a responsibility assignment matrix (RAM).

⁷ The duration of the workshop is suggested as an indication. It does not include the preparatory and formalisation work to be carried out upstream and downstream.

At this step, it is essential to identify who is the person accountable for accepting the residual risks at the end of the study.

Then define the **timeframe** of the study (durations of the operational and strategic cycles). These durations must be adapted to the project constraints and be consistent with the standards, legal and regulatory frameworks in effect. Ordinarily, for an information system accreditation, the generic durations are three years for the strategic cycle and one year for the operational cycle.

Aspects relating to project management such as the planning of the workshops to be conducted or resources constraints can also be addressed.

b DEFINE THE BUSINESS AND TECHNICAL PERIMETER

In a second step, you will list the missions, business assets and supporting assets regarding the studied object⁸. The questions that may be raised are:

- *What is the object of the study? What are its main missions, its purposes?*
- *What are the major processes and information that enable the studied object to carry out its missions?*
- *What are the digital services, applications, IT networks, organisational structures, human resources, premises, etc. which enable to carry out these processes or process this information?*

Start by listing all of the **missions** of the studied object, i.e. the end purposes and major goals of the latter (the way it participates in creating value, for example). According to the level of detail of the study, the missions to be identified can sometimes be intrinsic to the studied object but are generally those of the organisation of which the object is part of.

8 In order to carry out this activity, you can use the model suggested in methodological sheet no. 1.

In the same way, then list all of the **business assets** associated with the studied object, namely the information or processes deemed important, in the framework of the study, and that should be protected. The business assets represent the informational assets that a risk origin would have an interest in attacking in order to achieve its objectives (example: on-line reservation cancelling service, customer information, results of R&D work, deployment phase of a project, know-how in designing aeronautical parts, etc.).

At this stage, the objective is not to be exhaustive but rather to limit the number of business assets in order to retain only those identified as essential or sensitive. Proceeding as such makes it possible to keep a certain agility in the study and to reduce the work to a useful and acceptable level. In order to reach this end, you can for example:

- consider sets of information rather than isolated pieces of information;
- rank the business assets according to their security needs (availability, integrity, confidentiality, etc.)⁹.

In terms of volume, 5 to 10 business assets generally form a base that is sufficient for orienting the rest of the study. The business assets that are not selected can however inherit the measures taken to protect the other business assets.

⁹ To rank the business assets, it is possible to judge whether their security needs are "very high", "notable" or "negligible". It is also possible for the assessment of the security needs of a business asset to use scales for scoring, for example those with 3 or 4 levels used in the examples of the EBIOS 2010 method. However, the objective is not to seek an absolute value but rather a relative position of the business assets in relation to one another.

Then list the supporting assets regarding each business asset. These are elements of the information system on which the business assets are based. For this, use the mapping of the organisation's information system¹⁰. You can structure your listing according to the main categories suggested in methodological sheet no. 2.

NOTE : at this stage, you can limit the identification of the supporting assets to the most important ones, for example one to three supporting assets for each business asset. They will then be supplemented during the drawing up of operational scenarios.

¹⁰ To construct it, it is possible to refer to guide from the French National Cybersecurity Agency, ANSSI, *Mapping the information system - How-to guide in 5 steps*, 2018

EXAMPLE : Biotechnology company manufacturing vaccines.

MISSION	IDENTIFY AND MANUFACTURE VACCINES		
DENOMINATION OF THE BUSINESS ASSET	Research & development (R&D)		
NATURE OF THE BUSINESS ASSET (PROCESS OR INFORMATION)	Process		
DESCRIPTION	Vaccine research and development activity requiring: ■ the identification of antigens; ■ the production of antigens (attenuated live virus, inactivated virus): fermentation (harvest), purification, inactivation, filtration, storage; ■ preclinical assessment; ■ clinical development.		
ENTITY OR PERSON RESPONSIBLE (INTERNAL/EXTERNAL)	Pharmacist		
DENOMINATION OF ASSOCIATED SUPPORTING ASSET(S)	Desktop application servers (internal)	Desktop application servers (external)	Antigen production systems
DESCRIPTION	Desktop application servers storing all of the R&D data	Desktop application servers storing a portion of the R&D data	Set of IT equipment and machines that make it possible to produce antigens
ENTITY OR PERSON RESPONSIBLE (INTERNAL/EXTERNAL)	IT department / Information management team	Laboratories	Laboratories

Manufacturing vaccines	Traceability and control
Process	Information
Activity consisting in : ■ filling syringes (sterilisation, filling; labelling); ■ conditioning (labelling and packaging).	Information enabling to ensure the quality control and the batch release (examples: antigen, aseptic distribution, conditioning, final release...)
Production manager	Quality Manager
Production systems	Desktop application servers (internal)
Set of IT equipment and machines that make it possible to produce vaccines on a large scale	Desktop application servers storing all of the data regarding traceability and control, for the various processes
IT department / Information management team + Equipment suppliers	IT department / Information management team

NOTE: during this step, you may need to identify the business assets or supporting assets placed under the responsibility of entities that are outside your organisation. These elements can be included in workshop 3, when creating the ecosystem digital threat mapping.

c IDENTIFY THE FEARED EVENTS

Identifying and characterising the **feared events** (FE) enable the stakeholders to objectively compare the importance of the missions and the business assets while becoming aware of the security issues. In EBIOS Risk Manager, feared events are associated with business assets and reveal a harmful breach for the organisation. The degree of harm or impact is assessed according to a severity scale that makes it possible to rank feared events.

In order to reveal the FEs, you can, for each business asset listed in the preceding step, conduct research on the harmful effects subsequent, for example, to a breach:

- affecting the availability of the business asset (example: inaccessible information, total or partial interruption of service, impossibility to conduct a phase of a process);
- its integrity (example: forgery or modification of information, function creep of a service, alteration of a process);
- its confidentiality (example: disclosure of information, unauthorised access to a service, compromising of a secret);
- its traceability (example: loss of traceability of an action or of a modification of information, impossibility to track the chaining of a process);
- and more globally the quality of service and the performance that the business asset must satisfy.

Estimating the severity of each FE depends on the criticality of the business asset with regards to:

- the missions of the organisation;
- the regulations;
- the nature and the intensity of the direct impacts, and even indirect impacts.

Methodological sheet no. 3 is proposed to help you carry out this activity.

NOTES

- A feared event is described in the form of a short expression or scenario that allows for an easy understanding of the harm linked to reaching the business asset concerned. The prior assessment of the security needs can help in estimating the severity.
- For feared events (FE) that affect availability, we recommend that you specify beyond which loss of service the severity mentioned is reached (example: unavailability of the service for a duration exceeding 2 hours, impossibility to distribute data flows greater than 1 Mbps). This approach will in particular enable you to anchor in your risk assessment the notion of degraded operating mode.
- In order to estimate the severity, consider all of the possible types of impacts – internal, external, direct, indirect – in order to push the stakeholders into considering impacts of which they may have never initially thought of.
- At this stage, the FEs are identified from the organisation's view point, outside any attack scenario. They will then be useful in developing strategic scenarios (workshop 3), from the attacker's view point, and can be updated in this framework.

EXAMPLE : biotechnology company manufacturing vaccines.

The scoring of the severity of the impacts is carried out based on the following matrix:

SCALE	CONSEQUENCES
G4 CRITICAL	Incapacity for the company to ensure all or a portion of its activity, with possible serious impacts on the safety of persons and assets. The company will most likely not overcome the situation (its survival is threatened).
G3 SERIOUS	High degradation in the performance of the activity, with possible significant impacts on the safety of persons and assets. The company will overcome the situation with serious difficulties (operation in a highly degraded mode).
G2 SIGNIFICANT	Degradation in the performance of the activity with no impact on the safety of persons and assets. The company will overcome the situation despite a few difficulties (operation in degraded mode).
G1 MINOR	No impact on operations or the performance of the activity or on the safety of persons and assets. The company will overcome the situation without too many difficulties (margins will be consumed).

The company has listed a portion of the feared events in the following table:

BUSINESS ASSET	FEARED EVENT	IMPACTS	SEVERITY
R&D	Loss or destruction of analyses and research information resulting in a high impact, in particular on the company's future marketing authorisation procedure	■ Impacts on the missions and services of the organisation ■ Impacts on the costs of development ■ Impacts on the organisation's governance	3
	Alteration of analyses and research information resulting in an erroneous vaccine formula	■ Impacts on the safety or on the health of persons ■ Impacts on the image and trust ■ Legal impacts	3
	Leaking of the company's analyses and research information	■ Impacts on the organisation's governance ■ Financial impacts	3
	Interruption of the vaccine test phases for more than one week	■ Impacts on the missions and services of the organisation ■ Financial impacts	2
Manufacturing vaccines	Leaking of the company's know-how regarding the process for manufacturing vaccines and their quality tests	Financial impacts	2
	Interruption of the vaccine production or distribution for more than one week during the peak of the epidemic	■ Impacts on the safety or on the health of persons ■ Impacts on the image and trust ■ Financial impacts	4
Traceability and control	Alteration of the quality control results leading to a sanitary non-compliance	■ Impacts on the safety or on the health of persons ■ Impacts on the image and trust ■ Legal impacts	4

d DETERMINE THE SECURITY BASELINE

Determining the security baseline and the gaps assumes adopting a compliance approach, corresponding to the first two stages of the risk management pyramid. For this, you must identify all of the **security reference standards** that apply to the studied object.

These reference standards can be:

- healthy information system rules and security best practices : ANSSI's recommendation guides¹¹, the organisation's internal security rules, etc.;
- standards: ISO 27000 family, etc.;
- current regulations: you can refer to ANSSI's website¹² that lists a spectrum of regulatory texts in terms of digital security.

If the studied object is a system or a product that already exists, then assess the **implementation status** of the various reference standards listed, for example thanks to a colour indicator (green for "applied without restriction", orange for "applied with restrictions", red for "not applied", etc.) and clearly identify the **gaps**, as well as the causes of the latter.

11 www.ssi.gouv.fr/en/best-practices

12 www.ssi.gouv.fr/en/regulation

The security baseline can be formalised in a table, such as the one suggested hereinbelow for the purposes of illustration:

TYPE OF REFERENCE STANDARD	NAME OF THE REFERENCE STANDARD	IMPLEMENTATION STATUS	GAPS	JUSTIFICATION FOR GAPS
healthy information system rules and security best practices	guideline for a healthy information system	Applied with restrictions	Rule 8: identify each individual accessing the system by name and distinguish the user/administrator roles	Existence of a non-nominative admin account for the administration of the ERP (proprietary solution that does not allow for administration via another account)
			Rule 37: define and apply a backup policy for critical components	Backup policy currently being written by a working group

The gaps observed with respect to the security baseline will be included in the risk assessment conducted in the following workshops in order to identify the risks that they pose on the organisation. Security measures can then be defined during workshop 5 in order to limit them.

NOTE: the results of the risk studies conducted previously will be integrated in this step. Indeed, these studies permitted you to identify and to implement security measures. The latter are now part of the security baseline of your organisation and can be tested in the following risk assessment workshops.

WORKSHOP



Risk origins



1 / Objectives of the workshop

The purpose of workshop 2 is to identify the **risk origins** (RO) and their **target objectives** (TO), linked with the particular context of the study. The workshop aims to answer the following question: *who or what can infringe upon the missions and business assets identified in workshop 1, and for what purposes?*

The risk origins and the target objectives are then characterised and assessed in order to retain the most relevant ones. They will be useful for constructing scenarios for workshops 3 and 4.



2 / Participants in the workshop¹³

- Top management (at least during the last step of the workshop);
- Business teams;
- CISO;
- A specialist in analysing the digital threat will possibly supplement your working group, according to the team's level of knowledge and the desired level of precision.



3 / Outputs

At the end of the workshop, you must have established the following elements:

- the list of priority RO/TO pairs selected for the rest of the study;

¹³ The team can be supplemented with any person deemed useful.

- the list of the secondary RO/TO pairs that can be studied in a second step and which will, if possible, be the subject of attentive surveillance;
- a mapping of the risk origins.



4 / Steps of the workshop

This workshop, of variable length, can require 2 hours to one working day¹⁴ in order to:

- a. identify the risk origins and the target objectives;
- b. assess the RO/TO pairs;
- c. select the RO/TO pairs that are deemed as deserving priority in order to continue the analysis.



5 / How to proceed?

To conduct this workshop, you need to know the missions and the business assets of the studied object, coming from workshop 1.

The fine characterisation of the risk origins and of their target objectives requires having precise information on the state of the threat and must ideally turn to the sector involved: attackers or groups of attackers, assumed resources and motivation, methods of attack, the most exposed activities, etc. The daily cyber attack watch bulletins and the news regarding cybersecurity are also precious sources of information that make it possible to supplement and

¹⁴ The duration of the workshop is suggested as an indication. It does not include the preparatory and formalisation work to be carried out upstream and downstream.

specify the knowledge of the threat and to contextualise it.

Methodological sheet no. 4 directs you in organising this information so as to be able to take action based on it in order to assess the risks in the framework of workshop 2.

a IDENTIFY THE RISK ORIGINS AND THE TARGET OBJECTIVES

To conduct the workshop, you must ask yourself the following questions:

- *what are the risk origins that can harm the organisation's missions or high-level interests (sector-related, state-related, etc.)?*
- *what can the target objectives be for each risk origin in terms of the effects sought?*

One way of doing this is to review the categories of risk origins and target objectives suggested in methodological sheet no. 4: for each category of risk origin, determine what the attacker's profile is and what types of objectives the attacker wants to reach. The same risk origin can generate, where applicable, several RO/TO pairs, with target objectives of different natures.

NOTES

- One of the keys to success consists in searching varied categories of RO/TO pairs in order to have a differentiated panel of attacker profiles and target objectives from which the strategic scenarios of workshop 3 will be established. It is also important not to leave any blind spots: ensure that you cover the organisation's business assets as widely as possible.
- The target aimed by a risk origin can be beyond the sole perimeter of the studied object. In this case, the latter may be used as an intermediary to reach the TO or be subjected to collateral impacts due to its exposure to the risk.

EXAMPLE : biotechnology company manufacturing vaccines.

RISK ORIGINS	TARGET OBJECTIVES
Hacktivist	Sabotage the next national vaccination campaign by disturbing the production or the distribution of vaccines, in order to generate a psychological shock on the population and discredit the public authorities.
Competitor	Steal information by spying on the R&D work in order to obtain a competitive advantage.
Hacktivist	Disclose to the general public information on the way in which the vaccines are designed by collecting photos and videos of animal tests in order to rally the public opinion to its cause.
Cyber-terrorist	Alter the composition of the vaccines distributed during a national vaccination campaign for the purposes of bioterrorism.

b ASSESS THE RO/TO PAIRS

When the team has stopped producing new RO/TO pairs, you can assess the pertinence of each pair. The objective is to identify, in the pool of risk origins and target objectives listed, those that you feel are the most relevant. Although the feedback from participants can form a first basis for assessment, we also recommend that you use criteria and metrics for characterisation that will provide a certain degree of objectivity. The assessment criteria that are generally used are:

- the motivation of the risk origin to reach its target;
- its resources (financial, skills, attack infrastructures);
- its activity (is it active within the perimeter of the studied object, in the ecosystem, in the industry concerned, in a similar industry, etc.).

c SELECT THE RO/TO PAIRS SELECTED FOR THE REST OF THE ANALYSIS

Based on the preceding work, you can then finalise the workshop by selecting the RO/TO pairs for the rest of the study. One of the choice criteria is obviously the level of relevance assessed in the preceding step. Favour RO/TO pairs that are sufficiently distinct from one another and that will likely affect different business assets and supporting assets. In terms of volume, 3 to 6 RO/TO pairs generally form a base that is sufficient to develop strategic scenarios.

EXAMPLE : biotechnology company manufacturing vaccines.

RISK ORIGINS	TARGET OBJECTIVES	MOTIVATION	RESOURCES	ACTIVITY	PERTINENCE
Hacktivist	Sabotage the national vaccination campaign	++	+	++	Moderate
Competitor	Information theft	+++	+++	+++	High
Hacktivist	Disclosing information on animal tests	++	+	+	Low
Cyber-terrorist	Altering the composition of vaccines for bioterrorist purposes	+	++	+	Low

The working group will retain as a priority the pairs with high and moderate pertinence, and will initially set aside the cyber-terrorist threat and that linked to hacktivists who want to disclose information on animal tests, which are deemed to be less significant.

WORKSHOP



**Strategic
scenarios**



1 / Objectives of the workshop

The ecosystem includes all of the stakeholders that orbit the studied object and participate in carrying out its missions (partners, subcontractors, subsidiaries, etc.). More and more cyberattack *modus operandi* leverages the most vulnerable links in this ecosystem in order to reach their target (example: affecting the availability of a service by attacking the Cloud service supplier, booby-trapping the logistics supply chain of servers that facilitate sensitive data exfiltration).

The objective of workshop 3 is to obtain a clear view of the ecosystem, in order to identify the most vulnerable stakeholders in it. This will then entail building high-level scenarios, called **strategic scenarios**. These scenarios are attack paths that a risk origin can use to reach its target (i.e. one of the RO/TO pairs selected during workshop 2).

Workshop 3 is to be addressed as a preliminary risk study. This can lead to identifying the security measures to be applied with regards to the ecosystem. The strategic scenarios selected in workshop 3 form the base of operational scenarios for workshop 4.



2 / Participants in the workshop¹⁵

- Business teams;
- Functional architects;
- CISO (Chief Information Security Officer);

15 The team can be supplemented with any person deemed helpful.

- A specialist in cybersecurity will possibly supplement your working group, according to the team's level of knowledge and the desired level of precision.



3 / Outputs

At the end of the workshop, you must have established and identified the following elements:

- the ecosystem digital threat mapping and the critical stakeholders;
- the strategic scenarios;
- the security measures chosen for the ecosystem.



4 / Steps of the workshop

This workshop, of variable length, can require one to three half-days¹⁶ in order to:

- a. build the ecosystem digital threat mapping and select the critical stakeholders;
- b. develop strategic scenarios;
- c. define the security measures on the ecosystem.

¹⁶ The duration of the workshop is suggested as an indication. It does not include the preparatory and formalisation work to be carried out upstream and downstream.

5 / How to proceed?

To conduct this workshop, you need to know:

- *the missions and business assets of the studied object (workshop 1);*
- *the feared events and their severity (workshop 1);*
- *the risk origins and target objectives selected (workshop 2);*
- *the mapping of the information system and in particular its ecosystem view (see note).*

NOTE : the ecosystem view presents the various stakeholders with which the studied object interacts directly or indirectly in order to perform its missions and services. For the sake of efficiency, it can be limited to the interactions associated with the business assets. When possible, it is in your interest to use an existing mapping and to supplement it if needed. For more information, you can refer to the mapping guide proposed by ANSSI.

a BUILD THE ECOSYSTEM DIGITAL THREAT MAPPING AND SELECT THE CRITICAL STAKEHOLDERS

A stakeholder is said to be critical when it is likely to form a relevant vector for attack, due for example to its privileged digital access to the studied object, its vulnerability or its exposure. A well-informed risk origin (i.e. that knows the ecosystem of the target) will attempt, following a logic of least effort, to attack the stakeholder that appears to be the "weakest link". The objective is therefore to identify these critical stakeholders in order to include them in the development of strategic scenarios.

You will first assess the threat level induced by each stakeholder of the ecosystem on the studied object. It is preferable that the assessment of the stakeholders is based on criteria rather than solely on the judgement of experts or feedback.

You will then establish the **ecosystem digital threat mapping**¹⁷ on which all of the stakeholders of interest have to appear in terms of their threat level with regards to the studied object.

Finally, you will be able to select the critical stakeholders. Using risk acceptance thresholds will facilitate this selection work. A simple approach for creating the digital threat mapping and for selecting the critical stakeholders is suggested in methodological sheet no. 5. Stakeholders are assessed here based on the exposure criteria (dependency, penetration) and cyber reliability (maturity, trust).

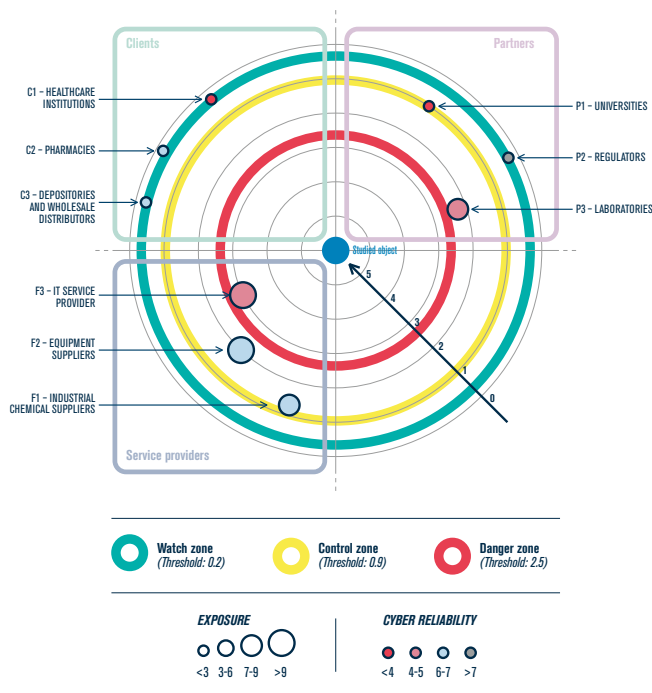
¹⁷ This tool will facilitate on the one hand selecting the critical stakeholders and on the other hand identifying the security measures to be implemented and to be written into contracts. The digital threat mapping is a variant, from a digital risk management standpoint, of the mapping of the information system. It is useful in conducting many projects and reflects your governance in terms of the digital risk management of the ecosystem.

EXAMPLE : biotechnology company manufacturing vaccines.

The team has decided to focus initially on the stakeholders external to the company. It has identified the following stakeholders:

CATEGORY	STAKEHOLDER
Clients	C1 – Healthcare institutions
	C2 – Pharmacies
	C3 – Depositories and wholesale distributors
Partners	P1 – Universities
	P2 – Regulators
	P3 – Laboratories
Service providers	F1 – Industrial chemical suppliers
	F2 – Production equipment suppliers
	F3 – IT service provider

The assessment of each stakeholder has made it possible to draw up the digital threat mapping hereinafter:



The team has retained F3 – IT service provider as a critical stakeholder. Stakeholders P3 and F2 are also selected as critical stakeholders. The other stakeholders were not retained as critical. After discussion with the CISO, although P1 and F1 are located in the control zone, they were not selected by the project manager, in light of the context and of the nature of the risk origins at stake¹⁸.

18 As indicated in the preamble, it shows that the analysis and the assessment carried out provide assistance in making decisions, but the latter reverts to project governance which can decide to set aside such and such threat element for contextual or policy reasons.

b DEVELOP STRATEGIC SCENARIOS

In the previous step, you constructed the ecosystem digital threat mapping and selected the critical stakeholders. The objective now is to imagine realistic high-level scenarios, indicating in what way an attacker could proceed to reach its target. It could for example go through the ecosystem or divert some business processes.

These so-called strategic scenarios are identified by deduction. In this approach, the analysis elements from the previous steps will provide precious assistance. In order to run this workshop, use as a starting point the RO/TO pairs selected in workshop 2. Then, for each RO/TO pair, engage the discussions by asking (yourself) the following questions from the standpoint of the attacker:

- *what is the organisation's business asset(s) that I have to aim for in order to reach my target?*
- *in order to make my attack possible or facilitate it, am I likely to attack the critical stakeholders of the ecosystem that have privileged access to the business assets?*

Once the most exposed elements have been identified, you can draw up the strategic scenario stemming from the RO/TO pair by describing the sequencing of the events generated by the risk origin in order to reach its target. Infringement on the business assets corresponds to **feared events** for the studied object while the events regarding the ecosystem are intermediate events.

Examples of events (intermediate or feared) of a strategic scenario: creation of an exfiltration channel from the service provider's infrastructure, modification of a critical parameter of the industrial process (high temperature threshold), denial of service attack of the cloud service supplier, deletion or alteration of a database, identity theft of a support service.

NOTE: the feared events that intervene in the strategic scenarios are to be found in the list of FEs established during workshop 1. However, contrary to the workshop 1, the FEs here are exploited from the standpoint of the attacker. As the standpoint is different, the list of FEs may need to be updated.

You can represent your scenarios in the form of **attack graphs** or directly on the ecosystem view of the mapping of the information system by superposing thereon the attack path(s).

You will then assess the level of **severity** of each scenario, with regards to the potential impacts associated with the feared events on the business assets.

NOTES

- Keep in mind that the end purpose is to identify the most relevant entry points, dissemination relays and attack vectors, in a logic of least effort, and to describe them in the form of events that correspond to intermediate goals for the attacker in order to reach their target. Avoid however developing strategic scenarios that are excessively detailed.
- In general, one to three attack paths for each RO/TO pair are enough to explore the relevant risk field. Take care to favour a variety of scenarios in which different critical stakeholders intervene and with various categories of business assets.

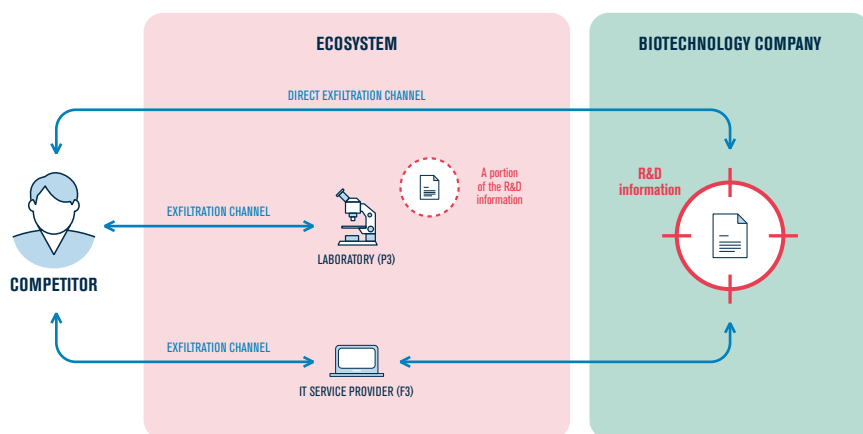
EXAMPLE : biotechnology company manufacturing vaccines.

The working group addressed first the RO/TO pair "A competitor wants to steal information by spying on the R&D work in order to obtain a competitive advantage" (see workshop 2). The three attack paths hereinafter were deemed relevant.

The competitor steals the research work:

1. by creating a data exfiltration channel that directly affects R&D's information system;
2. by creating a data exfiltration channel on the laboratory's information system, that holds a portion of the work (stakeholder P3 identified as a critical stakeholder in the previous step);
3. by creating a data exfiltration channel passing through the IT service provider (critical stakeholder F3).

The associated strategic scenario is shown hereinafter. It is of **severity 3 (serious)** according to the scoring carried out during workshop 1 on the feared events.

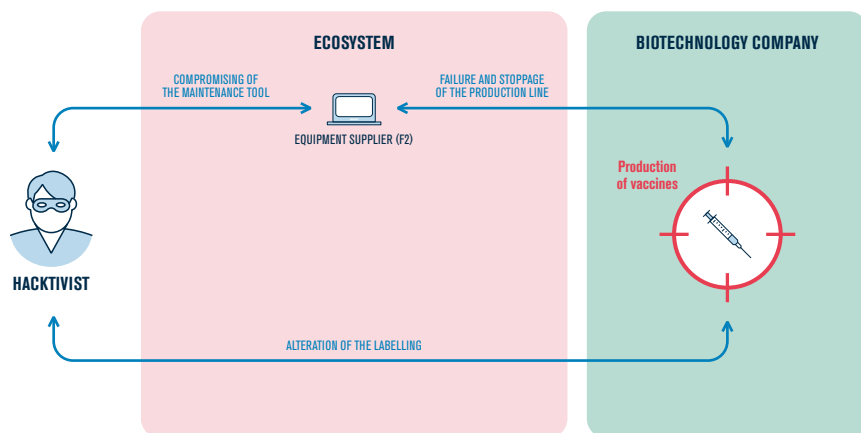


Then the working group focussed on the RO/TO pair: "A hacktivist organisation wants to sabotage the next national vaccination campaign by disturbing the production or the distribution of vaccines, in order to generate a psychological shock on the population and discredit public authorities". Two attack paths were identified as relevant.

The hacktivist disturbs the production or the distribution of the vaccines:

1. by causing an interruption of industrial production by compromising the maintenance equipment of the equipment supplier F2 (consequence: the manufacture of the vaccines is highly disturbed);
2. by modifying the labelling of the vaccines (consequence: the vaccines are not delivered to the correct location).

The associated strategic scenario is shown hereinafter. It is of **severity 4** (critical) according to the scoring carried out during workshop 1, as the most unfavourable case is considered since the incident occurs during the peak of an epidemic and lasts more than one week.



In summary, two strategic scenarios were selected:

RISK ORIGINS	TARGET OBJECTIVES	STRATEGIC ATTACK PATHS	SEVERITY
Competitor	Steal information by spying on the R&D work in order to obtain a competitive advantage	Three attack paths to be investigated. A competitor steals research work by creating a data exfiltration channel: 1. directly affecting R&D's information system; 2. on the information system of the laboratory (P3), that holds a portion of the work; 3. passing through IT service provider (F3).	3 Serious
Hackivist	Sabotage the next national vaccination campaign in order to generate a psychological shock on the population and discredit the public authorities	Two attack paths to be investigated. A hackivist disturbs the production or the distribution of vaccines: 1. by causing an interruption of industrial production by compromising the maintenance equipment of the equipment supplier (F2); 2. by modifying the labels of the vaccines.	4 Critical

c DEFINE SECURITY MEASURES ON THE ECOSYSTEM

The work carried out previously may have brought to light structural vulnerabilities linked to the internal and external stakeholders, that attackers will try to exploit in order to achieve their purposes. You may have also identified a scenario in which your organisation would be affected collaterally from an cyberattack targeting one of your partners. The aim of the last step of workshop 3 is looking for ways to reduce these risks and translating them into **security measures**.

The purpose of the security measures is to reduce the intrinsic threat level induced by the critical stakeholders (example: reduce the dependency on a subcontractor)¹⁹. They can also act on the unfolding of strategic scenarios.

NOTE: the security measures will likely have an impact on the governance of your organisation, and even on the one of your external stakeholders. Consequently, decision from the management is to be foreseen.

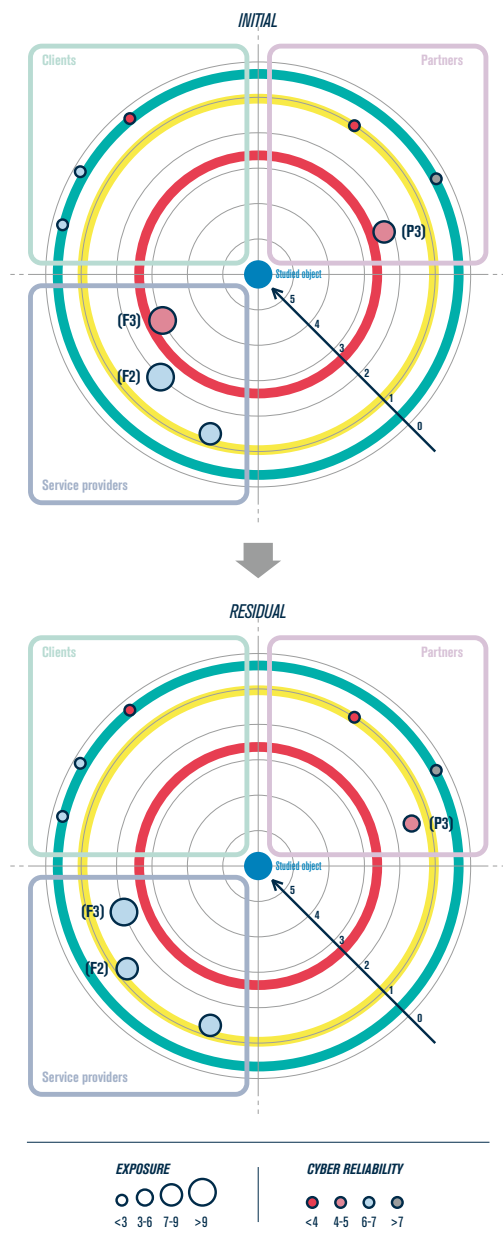
19 Simple rules are suggested in methodological sheet no. 6.

EXAMPLE : biotechnology company manufacturing vaccines.

Security measures have been defined in priority for the service providers F2, F3 and P3. The latter are indeed involved in strategic scenarios that are particularly problematic.

STAKEHOLDER	STRATEGIC ATTACK PATHS	SECURITY MEASURES	INITIAL THREAT	RESIDUAL THREAT
F2 Equipment suppliers	Interruption of production by compromising the maintenance equipment	Reduce the risk of booby-trapping the maintenance equipment used on the industrial system. Allocation of maintenance equipment administered by the IT department / Information management team and that will be made available to the service provider on the site (makes it possible to reduce the penetration of suppliers from 3 to 2).	2	1.3
F3 IT service provider	Information theft by passing through the IT service provider	Increase the cyber maturity of the service provider (2 → 3): ■ security audit (to be included in the contract); ■ following of the internal action plan. Reinforce the protection of R&D data. Solutions to be investigated: encryption, partitioning of the R&D network.	3	2
P3 Laboratories	Information theft on the information system of the laboratory	Decrease the penetration of the laboratories (3 → 2): limiting the data transmitted to the laboratories to the bare minimum needed (current bad habit of distributing "everything").	2.25	1.5

Applying the objectives hereinabove should make it possible within 9 to 12 months to reduce the risk, with a residual digital threat mapping as follows:



WORKSHOP



**Operational
scenarios**



1 / Objectives of the workshop

The objective of workshop 4 is to build operational scenarios. They diagram the methods of attack that the risk origins could use to carry out the strategic scenarios. This workshop adopts an approach similar to the one of the preceding workshop but focuses on the supporting assets. The operational scenarios obtained are assessed in terms of likelihood. At the end of this workshop, you will create a summary of all of the risks of the study.

The period to be considered for this workshop is the one of the operational cycle.



2 / Participants in the workshop²⁰

- CISO;
- IT department/Information management team;
- A specialist in cybersecurity will possibly supplement the working group, according to the team's level of knowledge and the desired level of precision.



3 / Outputs

At the end of the workshop, you must have established:

- the list of operational scenarios and their likelihood.

²⁰ The team can be supplemented with any person deemed useful.

4 / Steps of the workshop

This workshop, of variable length, can require one to three half-days²¹ in order to:

- a. develop the operational scenarios;
- b. assess their likelihood.



5 / How to proceed?

To conduct this workshop, you need to know:

- *the missions, business assets and supporting assets related to the studied object (workshop 1);*
- *the security baseline (workshop 1);*
- *the risk origins and target objectives selected (workshop 2);*
- *the strategic scenarios selected (workshop 3);*
- *the application and logical infrastructure views of the mapping of the IT system.*

a DEVELOP THE OPERATIONAL SCENARIOS

A successful attack is often the fruit of exploiting several flaws. Intentional attacks generally follow a sequenced approach. The latter exploits in a coordinated manner several vulnerabilities of an IT, organisational or physical nature. Such an approach based on the simultaneous exploitation of separate flaws can have heavy consequences even though the exploited vulnerabilities may seem insignificant when they are considered individually.

²¹ The duration of the workshop is suggested as an indication. It does not include the preparatory and formalisation work to be carried out upstream and downstream.

The operational scenarios defined in this workshop can be structured according to a typical attack sequence. Several models²² exist and can be used (example: the cyber kill chain model from Lockheed Martin). The approach must allow you to identify the **critical supporting assets** that can be used as vectors for entry or exploitation or as a propagation relay for the modelled attack. During workshop 5, the security measures will naturally concern these more particularly targeted supporting assets. However, the other supporting assets can inherit these measures.

Construct the operational scenarios by using as a base the strategic scenarios selected in workshop 3 and by using the mapping of the IT system. A good approach consists in representing your scenarios in the form of **graphs or attack diagrams**, useful for representing the attacker's methods of attack. You can use methodological sheet no. 7 in order to carry out this step.

NOTE: each strategic attack path selected in workshop 3 corresponds to an operational scenario that allows the risk origin to reach its target.

The diagram hereinafter shows the typical method of attack for a so-called "waterhole" attack of which the objective is to allow a risk origin to establish a data exfiltration channel.

22 A typical model is suggested in methodological sheet no. 7.

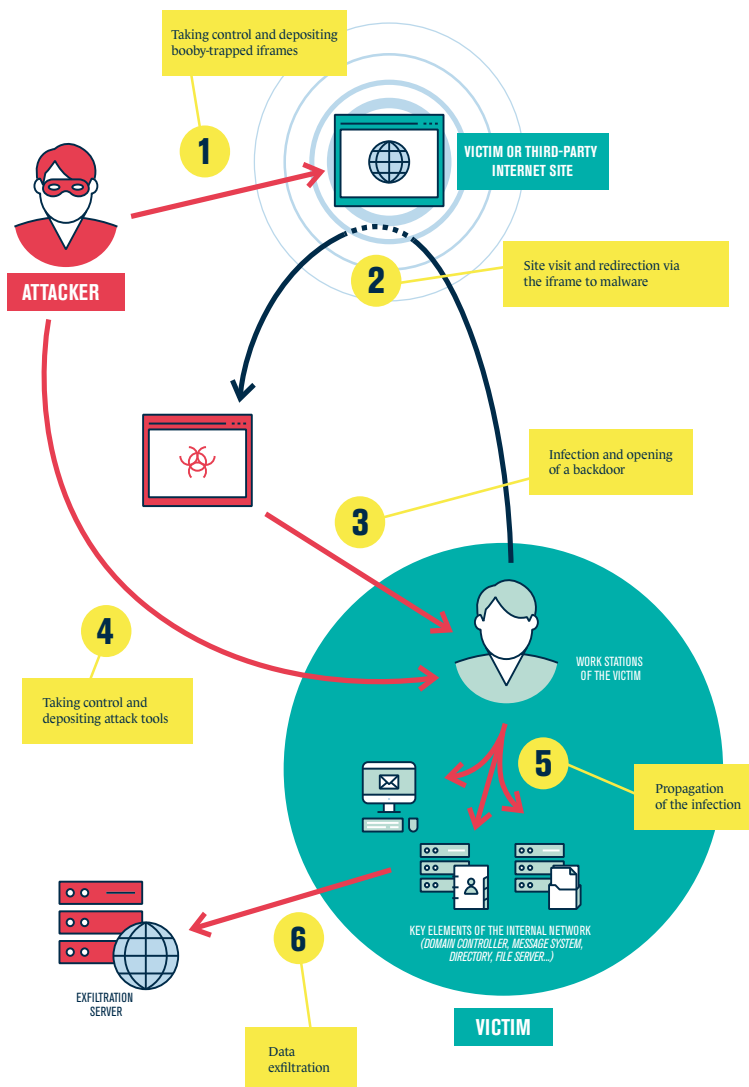


Figure 4 — Illustration of a so-called "waterhole" attack diagram

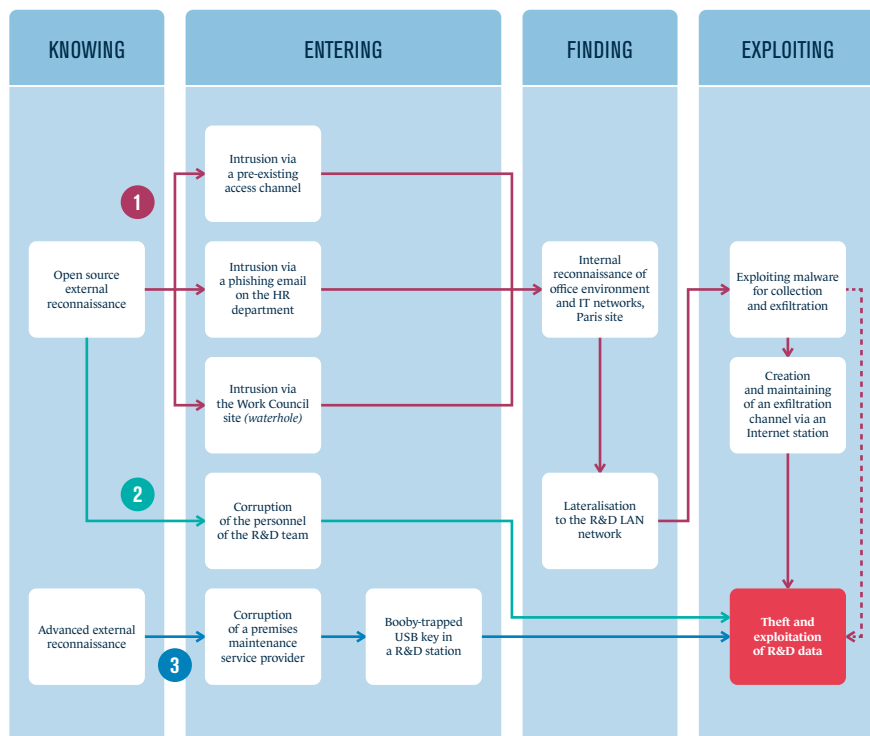
NOTE: in your operational scenarios, adjust the granularity of the method of attack in terms of the maturity of the organisation and the depth of analysis sought. This variable geometry approach makes it possible to include macroscopic elementary actions (example: attack of the "WannaCry" type) or more refined actions according to the level of detail desired for the sequence of the studied scenario or the sensitivity of the group of supporting assets considered.

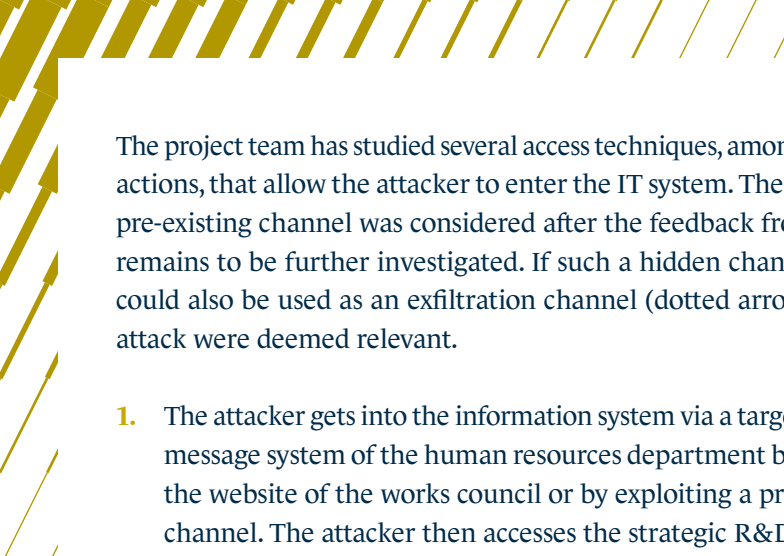
In order to avoid an excessive quantity of combinations of attack methods, give priority to those of least effort for the risk origin and which solicit a representative panel of the supporting assets present in the organisation.

EXAMPLE : biotechnology company manufacturing vaccines.

The project team has decided to represent the operational scenarios in the form of attack graphs. It decided to focus on carrying out a first operational scenario corresponding to a strategic attack path identified in workshop 3.

Operational scenario relative to the attack path "A competitor steals research work by creating a data exfiltration channel that directly concerns the information system of R&D (of the biotechnology company)":





The project team has studied several access techniques, among which collusion actions, that allow the attacker to enter the IT system. The exploiting of any pre-existing channel was considered after the feedback from the CISO, but remains to be further investigated. If such a hidden channel exists, then it could also be used as an exfiltration channel (dotted arrow). 3 methods of attack were deemed relevant.

1. The attacker gets into the information system via a targeted attack on the message system of the human resources department by booby-trapping the website of the works council or by exploiting a pre-existing hidden channel. The attacker then accesses the strategic R&D data due in particular to the absence of partitioning between the internal networks then exfiltrates by using the hidden channel or even a legitimate channel.
2. The attacker corrupts an employee of the R&D team who then easily recovers the information from his work station, since no supervision measure or action is carried out.
3. The attacker corrupts a member of the premises maintenance personnel and asks that person to plug in a USB key into an R&D workstation, that key being beforehand booby-trapped. This operation is facilitated by the fact that the maintaining of the premises takes place outside the working hours, the maintenance personnel has free access to the research department, and the USB ports are not subjected to any restrictions.

During the workshop, it was noted many times that the current lack of rigour in applying security patches substantially facilitated the exploitation of vulnerabilities.

b ASSESS THE LIKELIHOOD OF OPERATIONAL SCENARIOS

For each operational scenario, you will assess its overall likelihood, which reflects its probability of success or its feasibility.

NOTE: you may recall that the severity of the operational scenario corresponds to the severity of the associated strategic scenario, assessed during workshop 3.

Begin by assessing the **elementary likelihood** of each elementary action of your scenario. The latter can be estimated according to the judgement of an expert or using metrics. The assessment confronts on the one hand the assumed resources and motivation of the risk origin and, on the other hand, the security baseline of the studied object and the level of vulnerability of the ecosystem (exposed attack surface, structural and organisational vulnerabilities, capacities for detecting and reacting, etc.).

Then assess the **overall likelihood** of the scenario using elementary likelihoods. The assessment can, for example, focus on the method of attack of least effort for the risk origin. You can refer to methodological sheet no. 8 in order to carry out this assessment.

NOTE: you can also conduct a direct assessment of the overall likelihood of the scenario, without going through a detailed scoring of the elementary actions. Consider for example the likelihood of the various methods of attack as a whole. This express method however loses precision compared to assessing elementary likelihoods.

EXAMPLE : biotechnology company manufacturing vaccines.

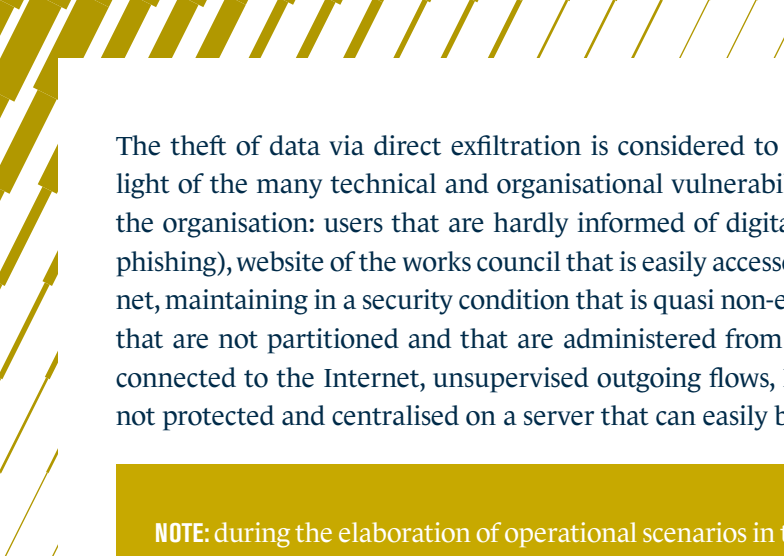
The five operational scenarios were developed during the preceding step by the project team (they will not be shown again here). They were assessed according to their level of likelihood, based on the following scoring grid:

OVERALL LIKELIHOOD SCALE OF AN OPERATIONAL SCENARIO

SCALE	DESCRIPTION
V4 Nearly certain	The risk origin will certainly reach its target objective by one of the considered methods of attack. The likelihood of the scenario is very high.
V3 Very likely	The risk origin will probably reach its target objective by one of the considered methods of attack. The likelihood of the scenario is high.
V2 Likely	The risk origin could reach its target objective by one of the considered methods of attack. The likelihood of the scenario is significant.
V1 Rather unlikely	The risk origin has little chance of reaching its objective by one of the considered methods of attack. The likelihood of the scenario is low.

STRATEGIC ATTACK PATHS (ASSOCIATED WITH OPERATIONAL SCENARIOS)	OVERALL LIKELIHOOD
A competitor steals research work by creating a data exfiltration channel that directly concerns R&D's information system	V3 Very likely
A competitor steals research work by creating a data exfiltration channel on the laboratory's IT system, which holds a part of the work	V2 Likely
A competitor steals research work by creating a data exfiltration channel passing through the IT service provider	V4 Nearly certain
A hacktivist disturbs the production of vaccines by provoking a stoppage of industrial production by compromising the maintenance equipment of the equipment supplier	V2 Likely
A hacktivist disturbs the distribution of vaccines by modifying their labelling	V1 Rather unlikely

The theft of R&D research data by the intermediary of the IT service provider is considered to be nearly certain. On the one hand, the service provider in question has high access rights to the biotechnology company's IT system and on the other hand the security of its IT system is weak. The combination of these aggravating factors makes an operation of intrusion and exfiltration very easy for an attacker with minimum engagement of resources.



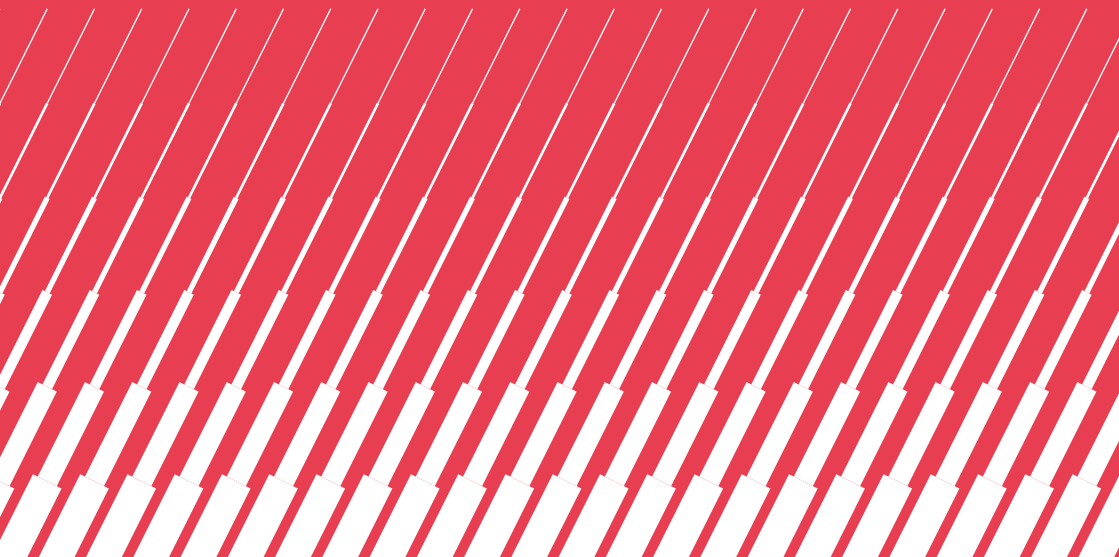
The theft of data via direct exfiltration is considered to be very likely in light of the many technical and organisational vulnerabilities observed in the organisation: users that are hardly informed of digital risks (example: phishing), website of the works council that is easily accessed from the Internet, maintaining in a security condition that is quasi non-existent, networks that are not partitioned and that are administered from stations that are connected to the Internet, unsupervised outgoing flows, R&D data that is not protected and centralised on a server that can easily be identified.

NOTE: during the elaboration of operational scenarios in this workshop, you may be led to update or supplement the strategic scenarios of workshop 3, for example if you identify a vulnerability that affects a stakeholder that was not considered or an alternative method of attack that you did not think of. The participants in workshop 3 will then be able to choose to retain or not the propositions put forth. Workshops 3 and 4 are thus supplied during successive iterations. Ensure however that you do not exceed two iterations in order to avoid complicating the analysis.

WORKSHOP



Risk treatment



1 / Objectives of the workshop

The purpose of this workshop is to create a summary of the risk scenarios identified and to define a risk treatment strategy. This strategy results in the defining of security measures, listed in a security continuous improvement plan (SCIP). The residual risks are then identified as well as the framework for following these risks.



2 / Participants in the workshop²³

The participants are the same as those for workshop 1:

- Top management;
- Business teams;
- CISO;
- IT department/Information management team.



3 / Outputs

At the end of the workshop, you must have defined the following elements:

- the risk treatment strategy;
- the summary of residual risks;
- the security continuous improvement plan;
- the framework for monitoring risks.

²³ The team can be supplemented with any person deemed useful.

4 / Steps of the workshop

This workshop, of variable length, can require two to four half-days of work²⁴ in order to:

- a. create the summary of the risk scenarios;
- b. define the risk treatment strategy and the security measures;
- c. assess and document the residual risks;
- d. set up the framework for monitoring risks.



5 / How to proceed?

To conduct this workshop, you need to know:

- *the security baseline (workshop 1);*
- *the strategic scenarios (workshop 3);*
- *the security measures regarding the ecosystem (coming from workshop 3);*
- *the operational scenarios (workshop 4).*

a CREATE A SUMMARY OF RISK SCENARIOS

First create a summary of the risk scenarios identified. A simple representation of these scenarios will facilitate their use in what follows.

These scenarios are most often positioned on a grid, a radar²⁵ or a Farmer diagram according to their levels of severity and likelihood. All of the representations adopted will form your **initial risk mapping**, i.e. before treatment.

²⁴ The duration of the workshop is suggested as an indication. It does not include the preparatory and formalisation work to be carried out upstream and downstream.

²⁵ Kiviati diagram.

EXAMPLE : biotechnology company manufacturing vaccines.



Risk scenarios:

R1: A competitor steals R&D information through a direct exfiltration channel

R2: A competitor steals R&D information by exfiltrating information held by the laboratory

R3: A competitor steals R&D information through an exfiltration channel via the IT service provider

R4: A hacktivist provokes the stoppage of the production of vaccines by compromising the maintenance equipment of the equipment supplier

R5: A hacktivist disturbs the distribution of vaccines by modifying their labelling

We suggest that you refine this summary work by representing your risk scenarios by risk origin and target objective (or according to any other criterion that seems relevant to you). The objective is to shed light and find analysis angles that are differentiated, able to assist in the understanding and the identifying of the most critical risk zones.

NOTE: covering the feared events identified in workshop 1 is an aspect to be considered in the summary work that you are conducting. This entails identifying if FEs of substantial severity – and the underlying business assets – were not left aside, resulting in a blind spot in the risk assessment. Review all of the FEs from workshop 1 and identify those that were not addressed in a risk scenario: according to their severity and the business assets concerned, you can then decide to conduct an iteration of workshops 2, 3 and 4 in order to supplement the list of risk scenarios. Draw up as needed a matrix of coverage between the feared events from workshop 1 and the risk scenarios treated in the risk assessment.

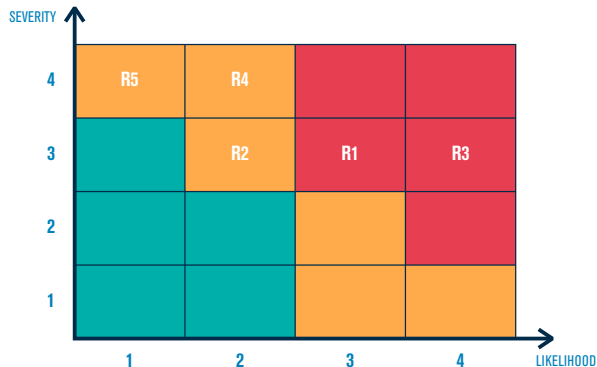
b DECIDE THE RISK TREATMENT STRATEGY AND DEFINE THE SECURITY MEASURES

For each risk scenario, agree on acceptance thresholds of the risk and level of security to be achieved in case of non-acceptance. This decision is formalised in the **risk treatment strategy**. We recommend the following acceptance classes, commonly used in risk management.

RISK LEVEL	ACCEPTABILITY OF THE RISK	DESCRIPTION OF THE DECISIONS AND ACTIONS
Low	Acceptable as is	No action is to be undertaken
Moderate	Tolerable under control	A follow-up in terms of risk management is to be conducted and actions are to be set up in the framework of continuous improvement over the medium and long term
High	Unacceptable	Measures for reducing the risk must absolutely be taken in the short term. Otherwise, all or a portion of the activity will be refused

It is possible for example to represent the risk treatment strategy according to the diagram hereinafter:

EXAMPLE : biotechnology company manufacturing vaccines.



Risk scenarios:

R1: A competitor steals R&D information through a direct exfiltration channel

R2: A competitor steals R&D information by exfiltrating information held by the laboratory

R3: A competitor steals R&D information through an exfiltration channel via the IT service provider

R4: A hacktivist provokes a stoppage of the production of vaccines by compromising the maintenance equipment of the equipment supplier

R5: A hacktivist disturbs the distribution of vaccines by modifying their labelling

Once the treatment strategy is validated for each scenario, define the associated **security measures** to treat it. This can be *ad hoc* measures linked to the context of use and threat, or reinforced measures among measures included in the security baseline. They supplement the measures on the ecosystem identified in workshop 3.

The identification of the risk treatment measures must result from the strategic and operational scenarios. Run through each scenario and ask yourself the following question: *what are the elementary phases or actions for which it would be relevant to reinforce the security, in order to make the task more difficult for an attacker and reduce their probability of success?* In the framework of an approach to analysing the asset, give priority to securing the elementary actions of which the likelihood is the highest as well as the strategic or operational nodes through which the risk origin could pass. This then entails giving priority to securing the critical supporting assets involved.

Document all of these treatment measures in a **security continuous improvement plan (SCIP)**, scheduled over time and structured²⁶. Each measure is associated with the person responsible, the main brakes and difficulties for implementation, the cost and the timeframe. The SCIP favours elevating the level of the organisation's IT system security maturity and allows for a progressive management of the residual risks.

26 Methodological sheet no. 9 proposes a typical structure for security measures.

EXAMPLE : biotechnology company manufacturing vaccines.

SECURITY MEASURE	ASSOCIATED RISK SCENARIOS	PERSON RESPONSIBLE	BRAKES AND DIFFICULTIES FOR IMPLEMENTATION	COST / COMPLEXITY	TIMEFRAME	STATUS
GOVERNANCE						
Reinforced awareness of phishing by a specialised service provider	R1	CISO	Validation from the Industrial Health and Safety Committee is indispensable	+	6 months	In progress
Technical and organisational security audit of the entire office environment IS by an audit service provider for information system security	R1, R5	CISO		++	3 months	To be launched
Integration of a warranty clause of a satisfying security level into contracts between providers and laboratories	R2, R3, R4	Legal team	Carried out as the contracts are renegotiated	++	18 months	In progress
Setting up of a procedure for reporting any security incident that takes place at the service provider's or at a laboratory	R2, R3, R4	CISO/ Legal team		++	6 months	To be launched
Organisational security audit of the key service providers and laboratories. Setting up and following up of consecutive action plans	R2, R3, R4	CISO	Acceptance of the approach by the service providers and laboratories	++	6 months	To be launched
Limiting the data transmitted to the laboratories to the strict minimum needed	R2	R&D team		+	3 months	Completed
PROTECTION						
Reinforced protection of the R&D data on the IS (solutions: encryption, partitioning)	R1, R3	IT department		+++	9 months	In progress
Reinforcing of the physical access control to the R&D office	R1	Security team		++	3 months	Completed
Allocation of maintenance equipment administered by the IT department and that will be made available to the service provider on the site	R4	IT department		++	9 months	To be launched
Reinforcing of the security of the industrial system according to ANSSI recommendations	R4, R5	CISO/IT department/ Security	Strategy and action plan to be defined and validated	+++	12 months	To be launched
Encryption of the data exchanges with the laboratories	R2	IT department	Identifying the encryption product and getting it accepted by the laboratories	++	9 months	To be launched
DEFENCE						
Reinforced management of the incoming and outgoing flows (IDS probe). Analysis of event logs using a tool.	R1	IT department	Purchase of a tool, budget to be allocated	++	9 months	To be launched
RESILIENCE						
Reinforcement of the business continuity plan	R4, R5	Business continuity team		++	6 months	In progress

C ASSESS AND DOCUMENT THE RESIDUAL RISKS

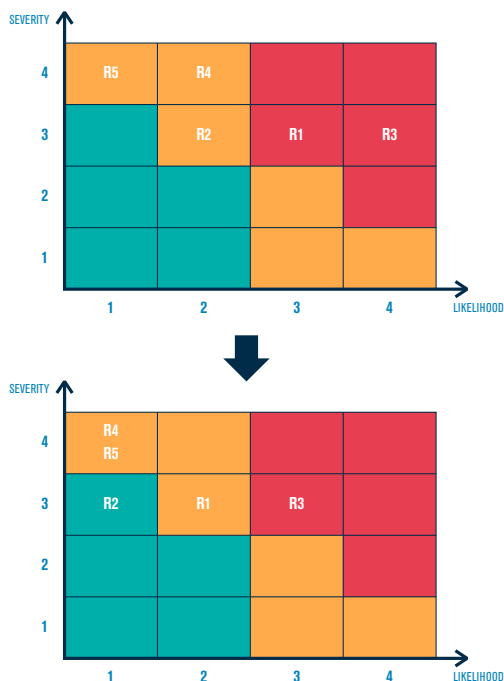
The assessment of the **residual risks (RR)** takes place after applying the treatment measures defined in the preceding step. You can for example document the residual risks according to the following model:

RR01 – DESCRIPTION OF THE RESIDUAL RISK: [...]		
Description and analysis of the residual risk: ■ Summary description (including the feared impacts) ■ Residual vulnerabilities that can be exploited by the risk origin ■ Other aggravating causes or factors (negligence, error, combination of circumstances, etc.)		
Feared events concerned: ■ Feared event 1 ■ Feared event 2 ■ [...]		
Existing and additional risk treatment measures: ■ Measure 1 ■ Measure 2 ■ [...]		
Assessment of the residual risk:		
Initial severity:	Initial likelihood:	Initial risk level:
Residual severity:	Residual likelihood:	Residual risk level:
Management of the residual risk: ■ Particular measures for monitoring and controlling the residual risk.		

We recommend that you represent the residual risks in the same way as the initial risk mapping. The residual risk mapping thus obtained can then be used as a reference when the formal review of the risks has to be conducted (during an accreditation commission meeting for example). It forms a decision-support tool for accepting residual risks.

NOTE: do not hesitate to associate with each major milestone of the security improvement plan (T0+3 months, T0+6 months, etc.) a residual risk mapping. You can thus present your upline management or an accreditation commission with the evolution of the residual risks over time, in view of the actions implemented.

EXAMPLE : biotechnology company manufacturing vaccines.



The management has decided to maintain the risk R3 at a high residual level, despite the application of the planned remedial measures. This risk is indeed considered to be particularly problematic, as the IT service provider is relatively opposed to setting up security measures. The latter indeed entail a rather profound change in its working methods. The solution considered for controlling this risk would consist therefore in entering the capital of this service provider in order to modify the governance in terms of digital security or in changing service providers.

On the other hand, the top management wants to place under surveillance the bioterrorist threat which is currently deemed to be not very relevant (see workshop 2), but the top management sees it as a major concern.

d SET UP THE FRAMEWORK FOR MONITORING RISKS

The management of the risks, in particular the monitoring of the risks, must be based on **steering indicators** in order to ensure for example the maintaining in security conditions. These indicators make it possible to verify the effectiveness of the measures taken and their suitability in terms of the state of the threat.

Once these indicators are listed, define or refine the continuous improvement process for security and the related governance (organisation, roles and responsibilities, associated committees). It is recommended to form a **steering committee** that meets every six months to address this ramping up or every twelve months at cruising speed in order to ensure follow-up of the indicators, progress with the SCIP and the change in risks.

Updating the risk study is done in compliance with the scheduled strategic and operational cycles. In case of major events questioning the relevance of the scenarios (emergence of a new threat, significant change in the ecosystem or in the studied object, etc.), the latter will be the subject of an update at the right level.

Bibliography

INTERNATIONAL STANDARD ORGANISATION, ISO 31000: 2018 – Risk Management – Principles and guidelines. ISO, February 2018.



INTERNATIONAL STANDARD ORGANISATION, ISO 27001: 2013 corr. 2 (2015) – Information security management systems – Requirements. ISO, 2015.



INTERNATIONAL STANDARD ORGANISATION, ISO 27002: 2013 corr. 2 (2015) – Code of good practices for information security management. ISO, 2015.



INTERNATIONAL STANDARD ORGANISATION, ISO 27005: 2011 – Information security risk management. ISO, June 2011.



ANSSI, IT hygiene guide – 42 measures to reinforce your IT system's security Guide, September 2017.

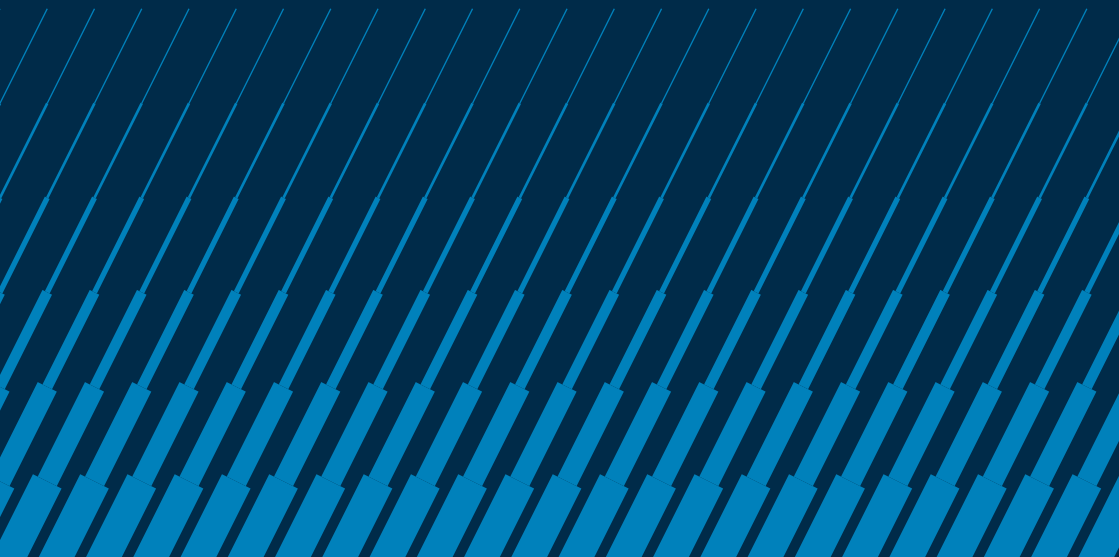


ANSSI, Map of the information system – Guide to drawing up in 5 steps. Guide, 2018.



ANSSI, Guides on cybersecurity for Industrial Systems. Guides, January 2014 and October 2016 for the case study.

Terms and definitions



ATTACK PATH

Section of code added to a piece of software in order to correct an identified vulnerability.



ATTACK SURFACE

All of the supporting assets on which the studied object is based or which interact with the latter, that could be used to carry out an attack. The higher the number of supporting assets or the more the latter have vulnerabilities that can be exploited by an attacker, the larger the attack surface.



BUSINESS ASSET

In the framework of the study, an important component for the organisation accomplishing its mission. This can be a service, a support function, a step in a project and any related information or know-how.

EXAMPLES : on-line back-up or reservation cancellation service, client information, supervision service, results of R&D work, personal data, deployment phase of a project, know-how in designing aeronautical parts.

NOTES :

- business assets represent the information assets that a risk origin would be interested in attacking in order to harm the studied object;
- in EBIOS 2010, this corresponds to the essential assets.



CRITICAL STAKEHOLDER

Stakeholder of the ecosystem that is likely to form a privileged vector for attack, due for example to its privileged digital access to the studied object, its vulnerability or its exposure to the risk. The critical stakeholders are identified in the ecosystem digital threat mapping.

CRITICAL SUPPORTING ASSET

Supporting asset that is deemed to be very likely to be targeted by a risk origin attempting to reach its target. Critical supporting assets are those that appear in the operational scenarios.



DENIAL OF SERVICE

A denial of service attack aims to render one or several services unavailable via the exploitation, for example, of a software or hardware vulnerability. The term distributed denial of service (or DDoS) is used when the attack makes use of a network of machines – most of the time compromised – in order to interrupt the targeted service or services.



ECOSYSTEM

All of the stakeholders with interactions with the studied object. Interaction means any relationship that takes place in the normal operation of the studied object. The risk origins are not considered *a priori* as stakeholders, unless they can affect the operation of the studied object.



ECOSYSTEM DIGITAL THREAT MAPPING

Visual representation (example: radar) of the digital threat level of the stakeholders of the ecosystem with regards to the studied object.



ELEMENTARY ACTION

Unitary action executed by a risk origin on a supporting asset in the framework of an operational scenario.

EXAMPLES: exploiting a vulnerability, sending a booby-trapped email, erasing trails, increasing privileges.

ELEMENTARY LIKELIHOOD

Likelihood of an elementary action identified in an operational scenario. It can be determined by the judgement of an expert or using scales. The assessment confronts on the one hand the assumed resources and motivation of the risk origin and, on the other hand, the security baseline of the studied object and the level of vulnerability of the ecosystem (exposed attack surface, structural and organisational vulnerabilities, capacities for detecting and reacting, etc.).



FEARED EVENT

A feared event is associated with a business asset and harms a security need or criterion of the business asset (examples: unavailability of a service, illegitimate modification of a high temperature threshold of an industrial process, disclosure of classified data, modification of a database). The feared events to be exploited are those of the strategic scenarios and relate to the impact of an attack on a business asset. Each feared event is assessed according to the level of severity of the consequences, using metrics.



INITIAL RISK

Risk scenario assessed before application of the risk treatment strategy. This assessment is based on the severity and the likelihood of the risk.



INTERMEDIATE EVENT

In the sequence of a strategic scenario, an intermediate event can be generated by the risk origin with regards to a stakeholder of the ecosystem for the purpose of facilitating reaching its objective.

EXAMPLES : creating an exfiltration channel from the service provider's infrastructure, denial of service attack of the cloud IT supplier of the target.

LIKELIHOOD

Estimation of the feasibility or of the probability that a risk occurs, according to an adopted scale (very low, rather unlikely, nearly certain, etc.).



MISSION

Function, end purpose, reason of existence of the studied object.



OPERATIONAL SCENARIO

Chain of elementary actions regarding the supporting assets of the studied object or of its ecosystem. Planned by the risk origin for the purpose of achieving a determined objective, operational scenarios are assessed in terms of likelihood



OPERATING MODE

Series of elementary events that the risk origin will probably have to carry out in order to reach its target. This terminology relates to operational scenarios.



PENETRATION TEST, PENTEST

Method generally consisting in simulating an attack by an ill-intentioned user, by trying several operating codes in order to determine those that give positive results. This is both a defensive intention (provide better protection) and an offensive action (attack one's own information system). The potential risks due to a poor configuration (infrastructure audit) or to a programming fault (product audit) are thus analysed.

RESIDUAL RISK

Risk scenario remaining after application of the risk treatment strategy. This assessment is based on the severity and the likelihood of the risk.



RISK

Possibility of a feared event occurring and that its effects affect the missions of the studied object. In the cyber context in which EBIOS Risk Manager fits, a risk is described in the form of a risk scenario.



RISK ASSESSMENT

Set of processes for identifying, analysing and assessing risks (ISO 31000:2018). In the EBIOS RM approach, this corresponds to workshops 2 (risk origins), 3 (strategic scenarios) and 4 (operational scenarios).



RISK LEVEL

Measurement of the extent of the risk, expressed by combining the severity and the likelihood.



RISK MAPPING

Visual representation (example: radar, Farmer diagram) of the risks stemming from the risk assessment activities.



RISK ORIGIN (RO)

Element, person, group of persons or an organisation that can generate a risk. A risk origin can be characterised by its motivation, its resources, its skills, its preferred methods of attack.

EXAMPLES : state services, hacktivists, competitors, vengeful employees.

RISK SCENARIO

Complete scenario, ranging from the risk origin to the target objective of the latter, describing an attack path and the associated operational scenario.

NOTE : in the framework of this guide, only digital risk scenarios of an intentional nature are considered.



RISK TREATMENT STRATEGY

The risk treatment strategy formalises the acceptance thresholds of the risk and level of security to be achieved in case of non-acceptance. It is carried out using the initial risk mapping: for each risk stemming from the risk assessment activities, the treatment strategy must define the acceptability of the risk (example: unacceptable, tolerable, acceptable). Usually, acceptability is directly deduced from the level of risk and the strategy is simply the formalisation of it. The role of the risk treatment strategy is to decide the acceptance of each risk in light of the assessment activities.



SECURITY ACCREDITATION

Validation by an accreditation authority that the level of security achieved by the organisation is compliant with the expectations and that the residual risks are acceptable in the framework of the study.



SECURITY CONTINUOUS IMPROVEMENT PLAN (SCIP)

The security continuous improvement plan formalises all of the measures for treating the risk to be implemented. It favours elevating the organisation's IT system security maturity and allows for a progressive management of the residual risks. The measures defined in the security continuous improvement plan relate both to the studied object and its ecosystem.

SECURITY MEASURE

Means of treating a risk taking the form of solutions or requirements that can be written into a contract.

NOTES :

- a control can be of a functional, technical or organisational nature;
- it can also act on a business asset, supporting asset, a stakeholder of the ecosystem;
- certain measures can be reinforced mutually by acting along complementary lines (governance, protection, defence, resilience).



SECURITY NEED

Security property to be guaranteed for a business asset. It reveals a security stake for the business asset.

EXAMPLES : availability, integrity, confidentiality, traceability.



SECURITY PATCH

Section of code added to a piece of software in order to correct an identified vulnerability.



SEVERITY

Estimation of the extent and of the intensity of the effects of a risk. The severity provides a measurement of the detrimental impacts perceived, whether direct or indirect.

EXAMPLES : negligible, minor, major, critical, maximum.

SOCIAL ENGINEERING

Unfair acquisition of information used to obtain property, service or key information from another person. This practice exploits human and social flaws of the target structure to which the target information system is linked. Using their knowledge, charisma or audacity, the attacker abuses the trust, ignorance or gullibility of the targeted persons.



SUPPORTING ASSET

Component of the information system on which one or several business assets are based. A supporting asset can be of a digital, physical or organisational nature.

EXAMPLES : server, telephone network, interconnection gateway, technical room, video protection system, team in charge of the project, administrators, R&D department.



STAKEHOLDER

Element (person, information system, organisation, or risk origin) with direct or indirect interaction with the studied object. Interaction means any relationship that takes place in the normal operation of the studied object. A stakeholder can be internal or external to the organisation to which the studied object belongs.

EXAMPLES : partner, service provider, client, supplier, subsidiary, related support service.

STRATEGIC SCENARIO

Attack paths going from a risk origin to a target objective and including the ecosystem and the business assets of the studied object. Strategic scenarios are assessed in terms of severity.



STUDIED OBJECT

Organisation, information system or product that is the object of the risk assessment.



TARGET OBJECTIVE (TO)

End purpose targeted by a risk origin, according to its motivations.

EXAMPLES : theft of information for lucrative or industrial spying purposes, diffusing an ideological message, take revenge on an organisation, generate a health crisis.



THREAT

Generic terms used to designate any hostile intent to do harm in cyberspace. A threat can be targeted or not on the studied object.



THREAT LEVEL OF A STAKEHOLDER (WITH RESPECT TO THE STUDIED OBJECT)

Provides a measurement of the risk potential that a stakeholder places on the ecosystem of the studied object, in light of its interaction with it, its vulnerability, its exposure to the risk, its reliability, etc.

VULNERABILITY

Fault, via malicious intent or thoughtlessness, in the specifications, design, carrying out, installation or configuration of a system, or in the way of using it. A vulnerability can be used by an operating code and lead to an intrusion in the system.



WATERHOLE

Booby-trap set up on a server of an Internet site that is visited on a regular basis by the targeted users. The attacker waits for their victim to connect to the server in order to compromise the latter. The booby-trapped Internet site can be a legitimate or a fake site.

Version 1.0 – November 2019

ANSSI-PA-048-EN

Open Licence (Etabl – V1)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75 700 PARIS 07 SP

www.ssi.gouv.fr – communication@ssi.gouv.fr – ebios@ssi.gouv.fr

