RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
RISK MANAGEMENT FRIMEORK

THE SECURITY ACCREDITATION GUIDE FOR INFORMATION SYSTEMS

COLLECTION
CYBER RISK MANAGEMENT

THE SECURITY ACCREDITATION GUIDE FOR INFORMATION SYSTEMS

PREAMBLE

Information systems[1] have become essential to the functioning of public and private entities.

Their misuse can lead to risks which may have catastrophic human, financial, legal, or reputational impacts.

The formal consideration and acceptance of these risks by an authority is referred to as 'security accreditation', and in a large number of cases is a regulatory requierement.

With the help of this guide, it seemed important to further understand and detail the process that organisations could follow to accredit their information systems.

This guide is intended for all persons intending to carry out, initiate, or support an accreditation procedure.

Written by ANSSI[2] in collaboration with DINUM[3] , it draws on years of development and support in the field of accreditation, and on the significant feedback provided by experts from the public service and private sectors.

This guide is meant to be accessible in its legibility and applicable to all information systems, from the simplest to the most complex, regardless of their criticality or exposure to sources of risk.

> NOTE: This guide is intended to provide support in the accreditation of information systems. It is not intended to replace any efficient method already established in your organization.

1. In the interest of simplicity, the term 'information system' here refers to any system which enables the processing of information, whether physical (computers, computer equipment), logical (software), or virtual (cloud/cloud system), and whatever its complexity or sensitivity.
2. The National Agency for the Security of Information Systems
3. Direction interministérielle du numérique

In an ever-changing digital world, the Security Accreditation Guide is bound to be regularly improved and developed. It is part of the "Cyber Risk Management" collection[4] intended to enhance our understanding of cyber risks.

It is complemented by method sheets allowing different typologies of information systems to be considered during the accreditation process.

4. Including the EBIOS RM risk analysis method (https://cyber.gouv.fr/la-methode-ebios-risk-manager), and MonServiceSécurisé (https://monservicesecurise.cyber.gouv.fr)

TABLE OF CONTENTS

1

BEFORE YOU START

THE NEW SECURITY ACCREDITATION DOCTRINE

The new security accreditation doctrine was devised by the French Cybersecurity Agency, alongside all of its interlocutors, to simplify and speed up the accreditation process.

Significant changes have been made and will be further detailed in this guide. For ***example***:

- Accreditation must be seen as the acceptance of business risks, by a business authority, for an organization.
- Three progressive levels of approach have been identified to allow efforts to be adapted to the criticality and exposure of the concerned information system.
- Only one type of accreditation: the notions of interim accreditation to operate (IATO), tests and accreditation to operate (ATO) disappear in favour of a singular type of accreditation. Only the validity period of the accreditation counts.
- Information systems which are little or non-critical and little or non-exposed can benefit from a simplified, trust-based accreditation process.
- The corpus of documents required for accreditation is greatly simplified.
- Accreditation committees may, in certain cases, be dematerialized.

1.1 A RISK-BASED APPROACH

Understanding the risks to which an organisation is exposed to is essential to anticipate and optimise decision-making. By adopting a risk-based approach in its strategy, an organisation can identify threats, become more resilient, and seize more opportunities.

To achieve this, it is crucial that all levels of the organisation – including managers and management teams – be sensitised and understand the risks which may affect their organisation.

The decision to use an information system within an organisation and its accreditation should be inscribed in this strategy.

1.2 SECURITY ACCREDITATIONS: WHAT ARE THEY?

The use of an information system can engender risks which may have serious impact on the activities of the organisation. Decision makers in the organisation must be aware of these risks and decide, with full knowledge of the facts, whether they wish to implement or sustain the information system.

Recommended by ANSSI for several years and made mandatory by a large number of official texts[5] , this decision is known as the 'accreditation decision[6].

It is therefore a prerequisite for any use of an information system

Any information system which is already in used without having been approved must be shut down or accredited within a reasonable period[7] of time.

> NOTE: A security accreditation is a formal act which commits the issuing authority.

5. See "Identifying the Applicable Regulations"..
6. The principle of approval exists in many countries and is sometimes referred to as 'homologation' or 'authorisation'
7. A reasonable period of time" refers to the time needed to submit an action plan to secure the information system to be approved.

Giving accreditation to an information system is useful to:

- ensure that the security risks associated with the use of the information system have been identified, and that the measures necessary to their handling are or will be implemented within a reasonable period of time;
- ensure that the regulations in force are ¬correctly applied;
- validate the action plan to be applied to the information system in order to strengthen its security;
- empower and engage the accepting authority and all associated

NOTE: Accrediting an information system strengthens its level of security and enhances the trust users, customers, and partners may have in its use.

The process for obtaining accreditation is referred to as the 'accreditation process'.

It must be adapted to each information system, its context of use, the nature of the data it processes, the security challenges it faces, and the threat landscape.

The work leading to accreditation begins with the design of the information system and ends with its decommissioning[8] .

The work is cyclical and iterative. An accreditation decision is made at each end-of-cycle.

NOTE: A security accreditation may be granted even if the work to secure the information system has not been completed.
An information system may be approved even if it¬ is subjected to risks which have not been dealt with but which are deemed acceptable by the authority.

8. The decommissioning of an information system consists in permanently shutting it down, dismantling the equipment of which it is composed and deleting the data which it contains.

1.3 UNDERSTANDING THE BACKGROUND OF THE ORGANISATION

Before looking at the information system, it is important to understand the organisation that will use it. This step is necessary to identify the context in which the organisation operates, its strategy, its challenges and, above all, the risks it faces.

The organization must ensure that the risks to which it is exposed are well identified, assessed, and addressed.

These efforts require the involvement of the right stakeholders9, who have a good overall vision of the organisation. Analyses such as PESTLE[9] or SWOT[10] used in management teams can be useful to identify the context in which the information system is used.

The context of the organisation can be taken into account to understand the risk appetite of the risk owner.

> NOTE: The level of risk an organisation is willing to accept depends heavily on its strategy.

1.4 ENGAGING MANAGEMENT TEAMS

Taking digital security into account in an organisation and for all the information systems it uses requires significant engagement from management teams, particularly with regards to:

- ensuring that security policies are established, understood, and implemented;
- ensuring that the human resources required for their application are available, trained, and committed;
- ensuring the allocation of the budget for securing information systems;

9. The PESTEL analysis describes an organisational strategy covering the political, economic, sociological, technological, legal, and environmental fields

10. SWOT is a strategic tool to identify the strengths, weaknesses, opportunities, and threats inherent to a given project, study, or information system

- communicating the importance of securing information systems by design, by raising awareness and training ;
- regularly improving processes related to the security of information systems;

1.5 UNDERSTANDING THE INFORMATION SYSTEM

The purpose of an IS and the security challenges it faces must be understood in order to identify its importance for the organisation.

The following questions should be answered:

- What is the business purpose of the information system?
- What other information systems is it connected to?
- What might the consequences for the organisation be, should the information system no longer be able to fulfil its mission?
- What might the impacts for the organisation be, should the information processed by the information system be lost, disclosed, or altered?

The challenges facing the information system must be understood:

- What are the strategic objectives of the information system? Social, political, contractual, financial impact, market share, informational, etc.
- Is there strong strategic or political pressure to launch the information system?
- What are the key dates of the project (e.g.: the deadline by which for putting into service)?
- Is the information system in competition with other information systems?
- Is the technology used by the information system new, and should it be launched before competitors?
- Has a significant investment been made in the design of the information system, and is a rapid return on investment requested by the Management director?

Simple answers to the questions must be provided in an appropriate format[11].

11. A simple presentation sheet of the information system must be clear, concise and affordable for all.

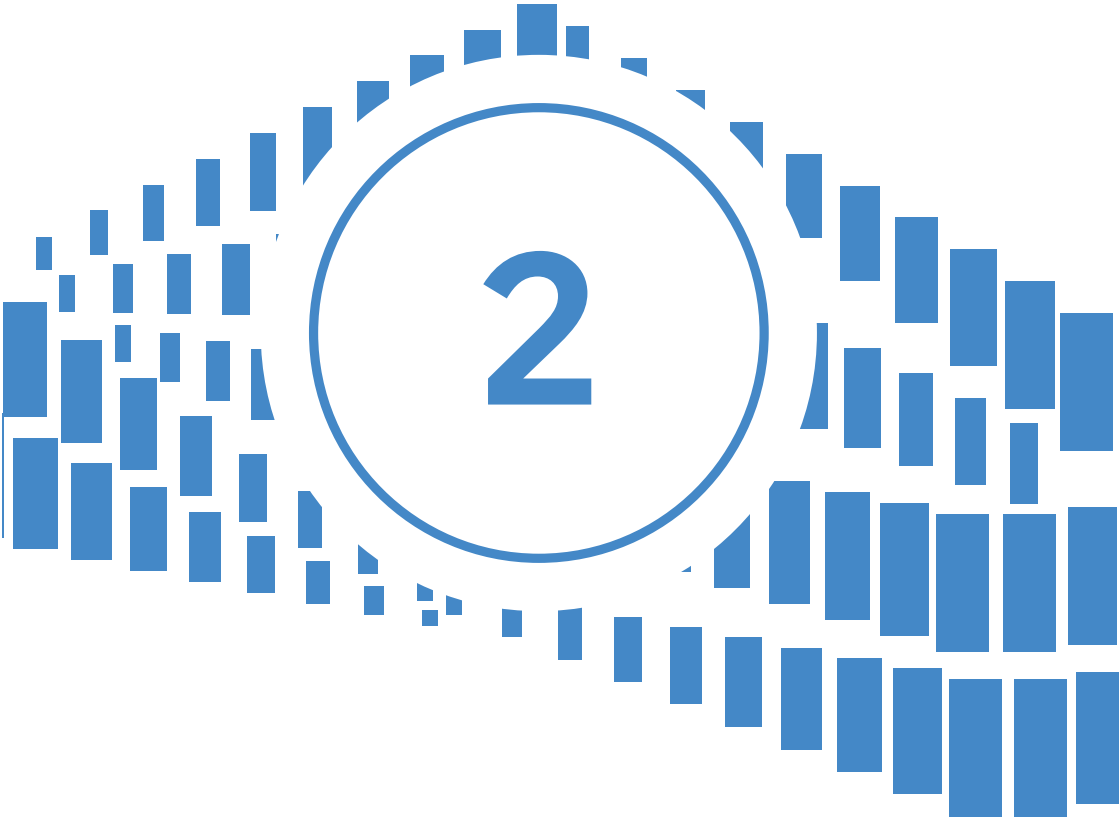
NOTE: For the organisation, understanding the information system in its context makes it possible to identify its criticality and the level of security to apply

THE ESSENTIAL:

Accrediting an information system ensures that the risks associated with its use are clearly identified and accepted at the highest level of an organisation (the Security Accreditation Authority).

An accreditation decision is a formal, regulatory act which commits the issuing authority. It stems from an approach which must start from the design of the information system - in the same way as its security. It requires the support of management teams.
An information system may be approved even if it is subjected to risks which have not been addressed but deemed acceptable by the authority. The risk acceptance can be temporary or definitive.
The level of acceptance of the risks to which an information system is exposed depends on the context of the organisation ¬employing it, and on its risk appetite.

SECURING THE INFORMATION SYSTEM



Actions to secure and accredit an information system are closely linked.

They must start with the design[12] of the information system and end with its decommissioning. They must be carried out as part of a project, which must be:

- punctuated by validation phases, corresponding to renewals ¬of accreditation;
- adapted to the information system, its context of use, the nature of the data processed, and security challenges.

NOTE: When regulations require accreditation, a procedure must be initiated. In any case, however, accreditation is strongly recommended by ANSSI for any critical information system in any given organisation.

2.1 ENFORCING SECURITY GOVERNANCE

Where possible, organisations must enforce the appropriate governance to facilitate efforts to secure information systems and their accreditation.

The three-line model (referred to as three "maturity" lines in this guide or as "defence" lines depending on the context) is suitable for this purpose.

12. See chapter "Identifying the level of the approval proces
13. Design/Security by Design
14. see "Controlling the digital risk" (https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance)

1st Maturity line	2nd Maturity line	3rd Maturity line	Owner
Operational (CIO)	Support (CISO)	Accreditation committee	External control

The first maturity line is made up of the operational teams. It is responsible for implementing and maintaining the measures provided by security policies, regulations, and action plans.

It conveys the appropriate information to the second line (e.g. Key Performance Indicators – KPIs). Generally, members of the IT team (CIO) are part of this line.

The second maturity line has a supporting role. It brings together risk specialists and provides the first line with the necessary support to improve the security of information systems.

It shares the security measures to be applied, and ensure that they are correctly applied by the first line.

It is responsible for steering information system audits and risk analyses.

The second line is generally responsible for security accreditation efforts. Chief Information Security Officers (CISO) are typically in charge of this.

Finally, **the third maturity line** must check that the information system is sufficiently secure to be used. It must, in close connection with the other maturity lines, collect the information required for accreditation, evaluate it, and submit an accreditation opinion to its authority. It manages the accreditation meeting (or commission). It should be noted that the third maturity line can be carried by the organisation's risk management team.

> NOTE: To achieve the common objective of securing and accrediting an information system, the tasks and responsibilities of the three maturity lines must be clear and well defined.The three lines must work closely together.

This three-line model allows for the separation of roles and the clarification of governance. It can be perfectly adapted to any organisation in possession of sufficient resources.

Ideally, these three roles should be held by different people.

In organisations where resources might not be sufficient, the roles identified can be performed by the same people. These can be internal or external to the organisation.

An additional maturity line may be used when control external to the organisation is required. In such cases, this line is responsible for verifying that the work carried out by the third line is sufficient to issue a security accreditation opinion.

It may be appropriate to present a responsibility assignment matrix (RACI) to identify the roles and responsibilities of each resource assigned to the project.

2.2 DEFINING THE PERIMETER OF THE INFORMATION SYSTEM

To conduct an accreditation, it is essential to identify the exact perimeter which needs an accreditation. Most of the time, the perimeter is an information system.

> NOTE: The perimeter of the information system to be approved comprises all of the components of the information system in which the information is processed, and for which an authority has been identified.

In this area of responsibility, the perimeter includes:

- which make it possible to produce, collect, store, process, and distribute the information;
- the services, applications, or software in charge of processing and exchanging information;
- physical equipment used to share information ¬with connected systems. This may be directly connected equipment or removable storage;
- the human resources associated with the information system. Users and administrators of the information system;
- geographical and physical locations. This may include data centers and any other place where the information system is located or used;
- and all of the equipment used to operate the information system, over which the business owner has control.

> NOTE: The perimeter of the information system must be clearly identified in technical and functional terms, and in terms of accountability.

It should be noted that the accreditation perimeter must, wherever possible, be isolated from its ecosystem via filtering mechanisms (firewall, diode), protocol breakdown, or any other means intended to slow down or stop a cyberattack.

The information system studied in the context of an accreditation process may be a combination of several complementary information systems with a common mission. In this case, we are referring to the "capability perimeter".

For example: two information systems – one used to manage employee leave and the other to manage salaries – may belong to the same accreditation area.

On the other hand, to facilitate efforts, it may be necessary to cut the perimeter down and carry out several accreditation perimeters.

This notably applies in cases where the information systems are different in nature or perimeter.

For example: an information system consisting of data hosting (file sharing), messaging, and telephony services may be subject to three separate accreditations.

Whatever the perimeter of accreditation, it must be clear and easily identifiable.

The choice of perimeter depends on the nature of the data processed and on its complexity.

Two information systems which have different protection or classification[15] levels have different security objectives. Therefore, they must be secured via two distinct accreditation processes.

It is not mandatory to have two separate accreditation procedures for an IS dealing with two different domains of the same protection or classification level.

The perimeter does not include components related to the information system which are not under the responsibility of the accreditation authority.

For example, in the case of an information system in PAAS mode, hosting servers are not part of the accreditation perimeter.

However, the use of these external components may lead to risks which will need to be identified and addressed during the risk analysis.

They belong to the ecosystem and need to be properly identified.

15. Public, personal confidential industrial confidential, and restricted data or restricted, secret and top secret classification.

16. UE, NATO, OCCAR…

17. PAAS : Platform As A Service is a set of resources made available by a third party who is responsible for it

Hosted information systems introduce a separation of responsibility between the data owner and the host. The perimeter of accreditation shall correspond to the perimeter of responsibility.

Accounting	SaaS	PaaS	IaaS	On-Prem
Data	x	x	x	x
Assets (PC and mobile)	x	x	x	x
Identities		x	x	x
Applications		x	x	x
System (OS)			x	x
Virtualization (device, network)			x	x
Physical host (+hypervisor)				x
Physical network				x
Data room				x

18. SaaS : Software as a Service, PaaS : Platform as a Service, IaaS Infrastructure as a Service

2.3 IDENTIFYING THE ECOSYSTEM

The ecosystem includes all of the components which are physically, technically, or organisationally interconnected with the information system¬ requiring an accreditation, but which are not part of its perimeter.

A component of the ecosystem is referred to as a 'brick' in the rest of this guide.

This may include:

- a connected information system;
- interconnection;
- an API or service used by the information system;
- a hosting or hosted platform;
- a workstation providing access to the information system;
- a data center housing the technical components;
- administrators not belonging to the accreditation perimeter;
- users outside of the organisation;
- etc.

Each identified brick provides one or more services[19] , data, or infrastructure.

The risks associated to their usage must be known.

> NOTE : Each brick must provide the level of security which corresponds to its criticality and to the trust level required by the information system under accreditation.

19. The services provided may, for example, be functional services specific to the business, services shared with a large number of customers, identity services, etc

For example:

- *An information system requiring a high level of availability must rely on an ecosystem with at least the same level of availability.*
- *An information system processing data which is required by regulation to be hosted in a sensitive area must ensure that the ecosystem complies with this requirement and is well located in that area.*

Guarantees may take the form of accreditation, certification, service level agreement, or any other information enabling the assessment of its safety and robustness.

> NOTE: The risks engendered by an ecosystem need to be identified and addressed.
> An ecosystem which provides the sufficient guarantees should, in theory, reduce the likelihood of these risks.

It should be noted that the information system – the object of accreditation – has likely been designated as a stakeholder in the 'ecosystem' of another interconnected information system.

It should therefore also provide it with the necessary guarantees to prevent weakening its own ecosystem.

Where possible, it is recommended that safeguards between bricks be formalised in a service contract detailing the security commitments[20] and requirements[21] of each party.

> NOTE: The security guarantees provided by each digital brick must be reviewed and maintained throughout the life cycle of the information system.

20. What brick assures "its customers" in terms of security

21. What brick asks of "its suppliers" in terms of security

It should be noted that information system's ecosystem may be made up of bricks which are themselves connected to other bricks. The origin and security level of these other bricks must be verified.

The boundary between perimeter and ecosystem is not always easy to identify.

The perimeter comprises all of the objects which directly enable the information system to function, and which are under the responsibility of the accreditation authority.

The ecosystem includes all of the objects which are used by the information system but which are not under the responsibility of the accreditation authority, because the accreditation authority does not have the authority to impose security measures on its ecosystem. The perimeter and its ecosystem can have a different mission or are separated in the interest of simplification.

The ecosystem must meet the minimum perimeter security requirements. The risks it engenders must be identified and addressed.

2.4 IDENTIFYING THE APPLICABLE REGULATIONS

It is crucial to identify national laws and regulations which require the accreditation or authorisation to operate of an information system.

2.5 COMPLIANCE WITH THE REGULATIONS

Regulations may define the (organisational and technical) security requirements applicable to information systems responsible for processing sensitive information.

As part of an accreditation process, specific features may be identified such as:

The accreditation authority:

- The accreditation perimeter, the citicity of the IS and the data sensibility are taken into account to identify the appropriate hierarchical level of accreditation authority.

The duration of the accreditation:

- An accreditation is not permanent and needs to be reviewed regularly. The duration of an accreditation may vary depending on the applicable regulations and must therefore be checked accordingly.

Audits:

- There are many ways of auditing an information system. Some may be mandatory, depending on the applicable regulations

Regulations are likely to evolve regarding the accreditation process and, as such, it is important to remain informed.

Failure to comply with regulation may result in liability on the part of the organisation's accreditation authority and in possible penalties.

2.6 IDENTIFYING THE SECURITY MEASURES TO BE APPLIED

The security measures to be applied must correspond to the information system's typology and specific security challenges.

The proper application of these measures helps to reduce known risks and to prevent or slow down cyberattacks.

The security measures to be applied are drawn from several sources:

- good practices in securing information systems;
- The relevant standards the organisation aims to implement;
- The mandatory regulation the organisation must be compliant to;
- the action plan born out of the risk analysis;
- security audit results;
- security events which occurred;
- the evolution of threats;
- and any other relevant sources.

Measures may cover aspects of governance, protection, defence, and resilience.

Information system security policies[22] may also introduce measures applicable to all of an organisation's information systems.

Its rules must be understood and applied.

> NOTE: In the event of a contradiction between a security policy and a current regulation, the regulation must be applied as a matter of priority.
>
> Where two regulations impose similar measures, the most restrictive measure must be applied.

22. The Information System Security Policy (ISSP) refers to the organisation's strategy for the security of information systems. It must be available, up-to-date and revised after each major change affecting information systems.

There are two types of measure:

- common measures to an organisation, e.g. user awareness-raising efforts, which must be implemented across the entire organisation, for all employees;
- specific measures to the information system under accreditation, e.g. mapping architectural documents which must correspond to the information system;

The measures must be proportionate to the risks they cover.

As such, if the application of the measure costs more than the risk it covers, it is conceivable not to apply it. This choice must be justified.

It is strongly recommended to monitor all of these measures by identifying those which may be:

- fully applied;
- partially or not applied;
- not applicable.

For each measure, it is important to justify its application or non-application[23] . When requested, the measure's return on investment (ROI) must be studied.

The monitoring of these measures (which can be compared to a statement of applicability[24]) can be useful to demonstrate the information system's compliance rate with said measures. Measures may also be monitored on a budgetary level.

It should be noted that all measures imposed by regulations must be applied where applicable.

23. The non-application of a measure may be justified by its greater human and financial cost than the impact on the business resulting from a security incident linked to the absence of the measure.

24. The Statement of Applicability is an important document required for the ISO27001 certification

For example, measures related to securing interconnections will not be applicable information systems which are not connected to any networks.

> NOTE: In order to be effective, a security measure must be applied or even improved throughout the life of the information system.

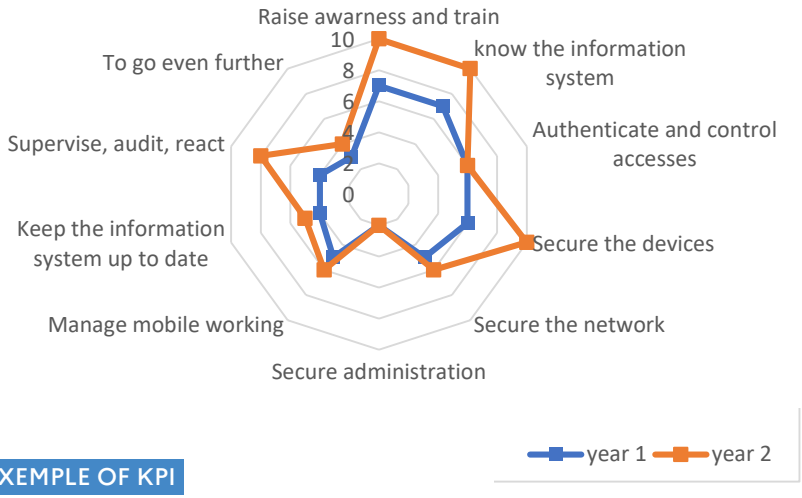
Monitoring efforts must be implemented by the second maturity line to ensure the correct application of the measure. This control may be supported by an audit.

In order to assess the efficiency of a security measure and monitor changes, it is strongly recommended to use **key performance indicators** (KPI).

These indicators – which can be widely spread to business decision makers – make it possible to set and track security objectives. They must be comprehensible and useful for any individual required to monitor the development of the information system. They can be used to quickly identify actions to be prioritised in order to strengthen the security of the information system.

A performance indicator must be relevant, specific, and achievable in relation to a target.

A graphic representation improves their readability



EXEMPLE OF KPI

Given that the objective of a measure may be interpreted, it is important to verify whether it is effective in relation to the objective set. In this case, a sample check is possible

2.7 DRAFTING A CARTOGRAPHY OF THE INFORMATION SYSTEM

Mapping is key to keeping the information system under control. When it is sufficiently detailed, it may significantly improve the teams' responsiveness in the event of an incident or attack affecting the information system.

It also facilitates the information system to be maintained in operational and security condition.

> NOTE: The accreditation's perimeter must be clearly identified in the mapping.

Maps need to be legible and understandable.

In general, a map is composed of three views (or visions), progressively focusing from business to technical

- The business view describes all of the main processes and information present on the information system. These are the 'business values' described in the context of the EBIOS Risk Manager methodology;
- The application view introduces the software components, services, and data flows which connect them;
- Finally, the infrastructure view illustrates the information system's physical and logical equipment, as well as all of the information enabling network communications – such as network addressing plans

Additionally, a more complete mapping may include the following elements:

- the list of profile types using or administering the information system;
- the list of strategies applied to the information system (GPO);
- information essential to the information system's maintenance in operational and security condition;
- procedures pertaining to the exploitation of the information system;
- procedures supporting the resilience of the information system.

25. See ANSSI guide https://cyber.gouv.fr/publications/mapping-of-the-information-system.

But also:

- the list of IT providers and suppliers contributing¬ to the information system's missions, including those of the ecosystem;
- the list of contracts related to the interconnected information system;
- the list and contacts of the internal and external partners involved in the information system;
- the inventory of the locations in which the information system is deployed or hosted;
- and any information useful to understand and to maintain the information system.

> NOTE: By definition, an information system's map must evolve alongside it. It should be updated with each major change in the information system.

In order to avoid the duplication of documents, it is recommended to keep only one mapping per information system.

The map must be dated and/or referenced.

The name of the person in charge of its maintenance must be clearly indicated. This person is responsible for setting the proper level of confidentiality and granting accesses exclusively on a need-to-know basis.

The map shall be stored in a location where it can be accessed in case of complete unavailability of the information system.

2.8 BUILDING OPERATING PLANS AND PROCEDURES

Operating procedures include all of the instructions for maintaining an efficient and secure information system throughout its use.

Operating procedures can cover a wide range of tasks, including:

- the management of incidents;
- the management of changes;
- the management of backups and restorations;
- the management of users and accesses.

Operating procedures must be drafted, tested, applied, -and updated according to a defined agenda and responsibility. They must be accessible to all concerned persons.
In order to draw up the list of procedures to be applied to an information system, ¬ it is essential to know its critical elements. To this end, mapping can prove extremely helpful.
A traceability mechanism must be implemented to ensure that they are correctly carried out by the operational teams.
Operating procedures should result in efficiency indicators, to facilitate the monitoring of the information system's general health within an overall scoreboard

	JANUARY	
	TODAY	**TARGET**
Data to backup	25To	25To
Success rate	87%	90%
Restore done	7	5

NOTE: In order to ensure the application of the operating procedures, it is recommended to improve and regularly evaluate them.

For example:

- If the information system and the data it manages are regularly backed up, have restoration tests been carried out? If so, are they successful?
- If user accounts are reviewed, what is the error rate? Is the review frequency adapted to the user audience?
- If the information system supports USB usage, what is the procedure for cleaning the support? Is it verified?
- If a business continuity process is defined, has it been tested?
- If the information system is located in a secure room, have physical accesses been checked?
- etc.

In order to maintain the security of the information system, specific plans must be applied:

- the "maintenance in operational condition" plan;
- the "maintenance in security condition" plan;
- the "resilience" plan.

NOTE: Plans must be drawn up by operational teams¬ (first maturity line).The second maturity line must ensure their implementation, relevance, and proper implementation

2.8.1 THE "MAINTENANCE IN OPERATIONAL CONDITION" (MOC) PLAN

Procedures to limit malfunctions which might prevent the information system from fulfilling its mission are part of the "maintenance operational conditions" plan.

The MOC brings together processes to ensure preventive maintenance, corrective maintenance, and the obsolescence of devices.

- Preventive maintenance includes all of the controls carried out before a breakdown occurs.

  For example, checking the free space remaining on a disk which needs to receive information;

- Corrective maintenance detailing the repair plan to be implemented after a malfunction.

  For example, the procedure for changing a damaged hard drive on an operational server

Other types of maintenance may be added to the operational maintenance plan, such as scalable and adaptive maintenance, which consists in integrating new functionalities into the information system according to the changes requested or its evolution in its environment.

Procedures for maintaining operational conditions must also include procedures for purchasing, for anticipating supply, for storing critical equipment, and for the management of obsolescence. Procedures for the decommissioning of part or all of the information system must also be detailed.

Procedures for the information system's maintenance in operational condition can encounter implementation issues which should be identified and accounted in an action plan.

For example, a shortage on a spare part that does not allow a replacement within the allotted time.

The main objective of the MOC is to minimise the information system's downtime and to ensure that it operates at a desired and appropriate level of performance.

Important performance indicators must be provided ¬to the second maturity line.

> NOTE : MOC procedures can be globally applied to a set of information systems

2.8.2 THE "MAINTENANCE IN SECURITY CONDITIONS" (MSC) PLAN

The aim of the procedures listed in the security maintenance plan is to correct any vulnerabilities detected on the information system before they can be exploited.

The MSC must detail the procedures necessary to patching the operating systems and software installed on the information system.

Three phases must be identified:

- **Monitoring** refers to the strategy implemented to ensure that new digital vulnerabilities are communicated to the persons responsible for the security of the information system ;
- **Reconnaissance** identifies any vulnerabilities which may impact the information system. This phase draw on an up-to-date map of the information system;
- The **implementation of corrective measures** is the step in which the affected components can ¬be regularly or urgently updated without disrupting the operation of the information system. In very critical environments, it must be preceded by a test procedure.

When patches cannot be applied for organisational or operational reasons, "trust bubbles" should be put in place in order to contain potential threats derived from unpatched vulnerabilities.

The "maintenance in security condition" plan must be built in collaboration with the operational and support teams responsible for the security of the information systems. It may be appropriate to draw up an global plan, common to the entire organisation.

> NOTE : The security maintenance plan may be merged with the operational maintenance plan

2.8.3 THE "RESILIENCE" PLAN

Despite the protection provided to enhance its security, an information system is not completely immune to security incidents which might cause its malfunction or shutdown. A resilience plan must therefore be implemented.

Resilience refers to an information system's ability to overcome alterations caused by a disruptive element and subsequently return to normal operation.

Any information system which is essential to the running of an organisation must be integrated into the Business Continuity Plan (BCP). This plan is defined as an organisation's ability to continue to deliver products and services, within acceptable timeframes and to a predefined capacity, during a disruption[26].

26. ISO22300:2021 (https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-3:v1:en)

A resilience document must detail the various measures envisaged in the event of a major event affecting the functioning of the information system.

Without being exhaustive, the resilience document must at least detail the following points:

- the maximum tolerable period of disruption (MTPD) of the information system before effects are irreversible for the organisation;
- the time needed to restart[27] the information system after an incident. This is an objective;
- crisis management procedures;
- the procedures for managing the business continuity and recovery plans.

The resilience plan must correspond to the criticality of the information system in the organisation. The more critical the system, the more detailed and tested the plan needs to be.
The plan must include a section on crisis management and, more specifically, on the management of cyber crises[28] .

NOTE : It is highly recommended not to repeat or detail resilience measures which are common to all of the organisation's information systems. A simple reference to the appropriate documents is sufficient.

27. RTO: Recovery Time Objective

28. https://cyber.gouv.fr/anticipate-and-gerer-a-cyber-crisis: Anticipating and managing a cyber crisis

2.9 IDENTIFYING AND HANDLING RISKS

Before an information system is put into service, the risks associated with its use must be identified, addressed, and accepted by a responsible authority.

> NOTE : An appropriate risk analysis method must be used, in line with the local security policy or as specified by the accreditation authorit.

The risk analysis must focus on the perimeter, which is the subject of the study, without omitting the risks associated with its ecosystem. It must clarify the information system's mission, as well as the main processes and information necessary to achieving said mission (business values).

As a reminder, a risk is the combination of a feared event and a threat scenario. The level of risk is assessed according to its severity and likelihood.

The analysis should identify, prioritise, and enable the management of risks[29] in order to make them acceptable to the accreditation authority.

The criticality and exposure of the information system has an impact on the depth of the risk analysis to be carried out: :

- for a system with low criticality and low exposure to digital threats, a study of its compliance with regulations and with the basic security measures[30] or recommendations issued by publishers is sufficient;

29. As a reminder, handling a risk requires accepting, reducing, transferring, or refusing it (see EBIOS RM method)

30. Basic security measure needs to be aligned with organisation policy

- For a more critical and/or exposed system, a risk analysis is recommended to identify the main risks faced by the information system ;
- Finally, for a system which is more critical to an organisation and/or exposed, a comprehensive risk analysis must be carried out in order to properly assess the intentional threat. Plausible attack scenarios must then be considered.

NOTE : Actions to address the risks must be carried out before the information system put in production, or planned within a reasonable period of time in agreement with the accreditation authority.

The risk treatment plan should be monitored and regularly updated, taking into consideration any new actions which might result from the evolution of the information system, its ecosystem, its context of use, regulatory framework and cyber threats. It must be integrated into a general action plan.

The plausibility of a risk evolves alongside the threats, the ecosystem, and the context in which the information system operates. It should be monitored via KPI.

2.10 AUDITING THE INFORMATION SYSTEM

Once security measures have been applied, the robustness of an information system against digital threats should be tested by means of a series of audits.

The perimeter chosen for these audits must correspond to the defined perimeter of the study.

The audit must be carried out by independent and trusted auditors who should have sufficient time to spend on the audits.

The audit and its perimeter must be authorised by the information system's manager and their hierarchy. In the case of classified systems, auditors must have the right level of habilitation.

Auditors should be free to submit their own scenarios.

It should be noted that regulations render certain audits mandatory:

- compliance audit: Does the information system comply with the applicable regulations?
- organisational audit: Is the human structure put in place to secure the information system sufficient and appropriate? Does it have sufficient means to guarantee its security? Is the documentation relevant?
- configuration audit: Are the components of the information system well configured to meet current security challenges?
- architecture audit: Is the technical implementation and organisation ¬of an information system consistent with its security objectives?
- technical audit: includes all audits in scope with technical elements (architecture, configuration, intrusion);

31. Non-exhaustive list

Other types of audit are possible and should be adapted to the nature of the information system, such as:

- code reviews;
- penetration tests ("pentests");
- bug bounties;
- electromagnetic radiation protection audit.

Audits allow the identification of minor and major non-compliances.

Audits verify the efficiency and effectiveness of the security measures put in place, and identify scenarios which might not have been considered during the risk analysis.

The vulnerabilities identified during an audit need to be addressed and included in the action plan.

The frequency of audits must correspond with:

- changes in stakes, context, or threat;
- the progress of the actions identified and corrected during the last audits;
- the availability of resources and allocated budgets.

Wherever possible, it is preferable to alternate the type of audit carried out to cover as many exploitable vulnerabilities as possible .

2.11 APPLYING THE ACTION PLAN

Improving the security of an information system is an ongoing process demanding constant effort that must be maintained from its design to its decommissioning.

All of these efforts reduce the risks faced by the system and need to be compiled into a single document – the action plan.

> NOTE: The action plan is a compilation of all actions undertaken to address regulatory non-compliances, to reduce identified and relevant risks, to mitigate vulnerabilities identified during audits, and to address security events and incidents.

In order to be actionable, the plan must identify realistic and useful actions.

The SMART method may be applied:

- The action must be specific to the risk to be reduced, or to the measure to be applied;
- The result of the action must be measurable;
- The objective of the action must be achievable and relevant;
- Finally, the action should be time bound.

It should be noted that an action may address several risks.

> NOTE: The action plan is the cornerstone of¬ continuous improvement and is intended to enhance the security of the information system.

A named owner, a complexity, a deadline, and a date of execution must at least be provided. The costs associated with carrying out the action may also be included in the plan.

EXAMPLE:

Action	Details	Justification	Owner	Complexity from + to +++	Due date
Remove useless network services	Remove telnet and http services from all servers, end user devices and network equipment (~120 devices)	Aligned with the "guideline for a healthy information system in 42 measures"	CIO : Mr or mrs X	+	

All information relevant to the monitoring of these actions should also be added.

Actions should be prioritised.

- Actions to address the most impactful and plausible risks should be carried out as a matter of priority.
- Actions with a high margin for improvement on the security of the information system should also be favoured.

THE ESSENTIAL:

Clear governance must be implemented in order to achieve the objective of securing and accrediting an information system. The three-line model of maturity makes it possible to distribute and control the tasks to be performed.
The perimeter of the information system and that of the ecosystem with which it communicates must be clearly defined.
The security measures drawn from regulations and security policies to which the information system is subject must be applied. The measures must be proportionate to the security challenges faced by the information system in its context.
In the case of critical[1] or exposed systems:

- Security (MSC) and Resilience (BCP) Operational Plans (MOC) must be identified and applied
- Risks associated with the use of the information system and its perimeter must be identified and addressed in a risk analysis.
- Audits must be carried out

An action plan laying out all of the measures necessary to bring the information system into compliance, or to reduce the risks associated with its use, must be implemented

32. The names of the levels are suggested but can be adapted to suit the organization. However, it is important to retain these three levels.

ACCREDITATION IN FOUR STEPS

The accreditation process enables the business authority to familiarise itself with the risks engendered by the concerned information system's use and, subsequently, to accept them. This authority is the accreditation authority.

Accrediting an information system authorises its use.

3.1 FIRST STEP:

FORMING THE ACCREDITATION COMMITTEE

In order to support the Accreditation Authority, a security advisory must be submitted by the Accreditation Committee – usually headed by the Chief Information Security Officer (CISO) or their representative.

The Accreditation Committee must be formed before the information system is put into service, and prior to each reaccreditation. It may be composed of:

- Business managers, to provide insight into the challenges associated with the use of the information system;
- The team responsible for the conception and design of the information system;
- The support team (IT), responsible for applying security ¬procedures when operating the information system;
- Auditors in charge of technical, organisational or configuration audits;
- "Experts" involved in assisting processes or conducting workshops;
- The risk manager and/or compliance officer of the organisation;
- Any interlocutor necessary to the submission of the security advisory.

NOTE : The head of the Accreditation Committee must ensure that the persons accompanying him are identified, available, and committed.

Contributors may be internal or external to the organisation. However, all persons involved in the accreditation process must be well informed. For classified systems, participants must have the appropriate level of habilitation.

NOTE : Each member of the Committee must be impartial with regards to the security opinion considered, whatever interests they may have in putting or maintaining the information system in operation.

3.2 SECOND STEP: IDENTIFYING THE ACCREDITATION PROCEDURE LEVEL

The accreditation process is the process by which a security advisory is collected, assessed, issued and presented to the authority.

The advisory must be constituted by the documentation drawn up by the support teams (first line of control).

The procedure level must be determined according to the criticality of the information system, and to its exposure to digital risk sources.

ANSSI suggests three accreditations procedures levels[32] (the more elevated level, the more reinforced is the security need)

- The simplified level is adapted to an information system with little or no criticality for its organisation. This may, for example, include a showcase website, an internal information system based on an isolated post, etc. The documentation requested is minimal;
- The intermediate level is intended for systems which are a little more critical or exposed to its sources of risk – systems responsible for processing personal data, for example;
- Lastly, the enhanced level is suitable for all information systems which are required to manage sensitive information and which are critical for an organisation.

Selecting a procedure level is a decisive step in the accreditation process and may therefore be subject to debate.

A questionnaire has been produced to assess the criticality and exposure of the concerned system in order to select the level.

It must be justified in the accompanying document, which should concisely present the information system.

33. A more comprehensive risk grid is available in the ANSSI EBIOS RM guide.

34. The Internet of Things (IoT) refers to physical devices that incorporate sensing and connec-

3.2.1 ASSESSING THE CRITICALITY OF THE INFORMATION SYSTEM

The assessment and definition of the criticality of an information system is often perceived as complicated endeavours. However, a simple and pragmatic approach framed as questions about the importance of the information system and the consequences of a potential failure can make this task more manageable :

- What are the impacts for the organisation or the users in the event of a total shutdown of the information system?
- What are the impacts for the organisation or the users if the data processed by the information system are disclosed to persons who should not have access to it?
- What are the impacts for the organisation or the users if the data processed by the information system are erased or corrupted, by accident or as a result of a malicious act?

In order to understand these consequences, it is necessary to assess the different impacts from different angles[33]:

- assets and persons;
- financial;
- legal and contractual;
- image;
- environmental;
- ...

The level of impact should preferably be evaluated using the organisation's existing criticality scales. Alternatively, the following scale may be used:

- minor impact: the impact is negligible;
- moderate impact: the impact has significant but surmountable consequences despite some difficulties;
- significant impact: the impact has important consequences which can be overcome with genuine difficulty;
- critical impact: the impact has serious and potentially irremediable consequences. The 'survival' of the organisation may be at stake.

tivity technologies. IoT devices are not known for their IT security.

3.2.2 ASSESSING THE EXPOSURE OF THE INFORMATION SYSTEM

The information system's exposure to digital risks can be ascertained by asking the following questions:

- Is the information system accessible via a network outside of the perimeter, e.g. the internet?
- Is the information system accessible only to a known population (employees, partners, etc.)?
- Can the information system be access by devices subjected to little or no control, e.g. IoT[34] or BYOD[35] devices.
- Are all places which provide access to the information system secure? Can the information system be accessed from home (teleworking)?
- Are the persons responsible for maintaining the information system trusted and using controlled devices?
- Is it easy to maintain the security of the information system?

These questions, which are not exhaustive, are intended to inform the Accreditation Committee on attack vectors which may be used by attackers.

35. Bring Your Own Device refers to the use of personal devices in a professional environment. This principle allows for greater flexibility in terms of equipment choice but creates additional management challenges.

36. This approach corresponds to the analysis of gaps in the security foundation carried out during the first workshop on the EBIOS RM method.

The following scale may be used to determine the exposure level of the information system¬, in a macroscopic view:

- zero: The information system must not be open on any network, and the transfer of information must be executed using trusted removable media. Access to the system is only possible for staff members who have been authorised by the entity;
- low: The information system is only open on controlled networks (e.g. on an intranet). Access to the system is only possible for staff members who have been authorised by the entity, and nomadic access is not permitted;
- important: The information system is indirectly opened on uncontrolled networks (e.g. by interconnecting SI with TLS tunnel). Access to the system is possible for staff members who have been authorised by the entity and/or for third-party staff members, and only some nomadic accesses are permitted;
- total: The information system is directly open on the Internet for all types of users and devices.

It should be noted that the information system's exposure to digital risk origins is linked to the threat level. There are three types of threats:

- The hacktivist or isolated threat, which brings together individuals with little means, using unsophisticated tools. They may, however, benefit from privileged access.
- The systemic threat can affect a large proportion of entities. Attacks associated to this threat are primarily profit-motivated. The perpetrators of these attacks typically use ransomware-like market tools.
- The strategic threat is illustrated by the conduct of persistent and targeted cyberattacks. They can be orchestrated by States or large organisations, motivated and resourceful.

NOTE : The exposure of an information system depends on its identified digital risk origins and on the associated threat level. .

3.2.3 SELECTING THE ACCREDITATION PROCEDURE LEVEL

The choice of a procedure level must be made by consensus among the members of the Accreditation Committee.

It should be noted that the chosen accreditation procedure level may change over the lifecycle of the information system.

The correspondence matrix below is intended to provide decision support in the final selection of the accreditation procedure to be implemented.

Identification of an accreditation procedure level

	Minimum exposure	Moderate exposure	Important exposure	Maximum exposure
	Intermediate	Reinforced	Reinforced	Reinforced
Important criticity	Intermediate	Intermediate	Reinforced	Reinforced
Moderate criticity	Simple	Simple	Intermediate	Intermediate
Minimum criticity	Simple	Simple	Simple	Intermediate

* The level of exposure (to sources of risk) must directly depend on the context in which the information system is used. It can be measured by trust in people or services with direct (e.g. via a network) or indirect access to it (e.g. by 'bouncing' on other information systems). The procedure level chosen directly influences the list of deliverables which make it possible to compile the accreditation file.

For example, a risk analysis is not necessary for an information system of minor criticality with near-zero exposure to digital risks. A compliance approach and the implementation of digital hygiene guides may cover the primary risks.

NOTE: The choice of an accreditation procedure level should not depend on the complexity of the information system, but rather on its criticality, its exposure to digital risk sources, and the level of threat faced.

The nature of the work to be carried out as part of the accreditation process is closely linked to the level of procedure chosen.

37. E.g. CIO, CISO, Business Manager

3.2.4 ASSEMBLING THE ACCREDITATION FILE

NOTE : The documentation which constitutes the accreditation file must be used to monitor and secure the information system, but it should not be specifically drawn up in furtherance of the accreditation procedure.

It should be noted that the documents in the accreditation file must be protected and classified as appropriate. They should only be accessible on a need-to-know basis.

NOTE : The documents which constitute the accreditation file make it possible to understand the information system and the risks associated with its use. They must be clear and useful to the teams in charge. Quality should therefore be given priority over quantity.

An accompanying document (or summary document) should be drawn up for the Accreditation Committee, presenting the information system and efforts implemented in order to secure it. Usually, this task is undertaken by the second line of control or by the business manager. This document should – at least – answer the following questions:

- What is the information system used for?
- What is the exact perimeter of the information system under accreditation?
- What is the business and technical context in which the information system is operating?
- What information does it process?
- What information flows enter and leave the information system?
- What is it made of? (Technology, Volumetry)
- How is it used? Who are its users?
- How critical is it to the organisation?
- What is its exposure to digital threats?
- What policies and regulations ¬must the information system comply with?
- What is the system's compliance rate with these policies and regulations?
- What procedures are in place to keep the information system operational and secure?
- How has the security of the information system been tested?
- What are the risks which might affect the information system, and what measures are being implemented to deal with them?
- What are the residual risks associated with the operation of the information system?
- Who administers the information system?
- What steps have been taken to improve the security of the information system?
- If the information system is already in use, what has happened since it was put into operation?

The accompanying document should be concise (one to two pages long) and should be updated for each Accreditation Committee.

The chosen level of procedure will have an impact on the information to be provided to the Accreditation Committee. For a critical information system, a reinforced approach will require the provision of more elements.

For example, a reinforced accreditation procedure requires a comprehensive risk analysis. This is not the case for a simplified procedure.

The following table lists the documents which the Accreditation Committee must collect and study, depending on the procedure level selected.

DOCUMENT TO BE SUBMITTED	Simplified	Intermediate	Reinforced
Executive summary (presentation of the information system, context and justification for the procedure	X	X	X
Technical architecture file	X	X	X
Compliance matrix	X	X	X
Risk analysis*	X	X	X
Operating procedure***		X	X
Operating maintenance plan***		X	X
Security maintenance***		X	X
Action plan	X	X	X
Resilience plan			X
Audits		X	X
History of the system information	X	X	X

*The compliance of information systems with the security base, the regulatory framework, and the security policies is studied during the risk analysis.

** In the context of an EBIOS RM risk analysis, all workshops are not necessary (e.g. only workshops 1 and 5 need to be carried out).

*** Generally common to all information systems of the organisation.

**** For information systems already in operation, the history should – at least – include its major security events and incidents, its technical and organisational changes, and its previous accreditations.

3.3 THIRD STEP: ASSESSING EACH COMPONENT OF THE ACCREDITATION FILE

The Accreditation Committee must ensure that security procedures are in place, that they correspond with the security challenges at hand, and that they are being properly implemented.

They must be documented.

The measures applied must be pragmatically analysed and assessed in order to reach a sufficient level of trust in the use of the information system.

It is often useful to organise Q&A sessions with the authors of the documents in order to go beyond the written ones.

> NOTE : The information exchanged during the accreditation procedure must be processed according to the appropriate level of classification by applying the regulation in force.

On the basis of the documents collected, the Accreditation Committee must be able to submit an opinion on the security of the information system.

The opinion must be based on the trust that the Committee obtains by analysing the documentation and conferring with its authors. The Committee must verify that all of the security steps have been followed.

It should be noted that the documentation must be adapted to the procedure and to the perimeter of the information system under accreditation.

It is not the role of the Accreditation Committee to produce documentation on the information system or to audit it.

3.3.1 SUBMITTING AN ACCREDITATION OPINION

The Committee should submit to the accreditation authority an accreditation opinion for the information system. This opinion must be justified.

Two cases may arise:

- **The information system is not ready for accreditation: Le système d'information n'est pas prêt à être homologué :**

  Despite all of the efforts implemented to secure the information system, its commissioning entails too many risks for the population. The information system must therefore not be used as it is. At this stage, there is no need to set up an Accreditation Committee. Nevertheless, it is important to communicate these risks to the different actors involved and to the accreditation authority.

NOTE : Not submitting a positive opinion on the security of a given information system is a strong message. It is indicative of a lack of maturity for this specific system. This opinion may enable the allocation of human and financial resources.

- **The information system is ready for accreditation:**

  The risks associated with the use of the information system have been identified and are being addressed to make their degree of plausibility acceptable; or

  The challenges facing the information system require that authorisation be granted, even if its security is not satisfactory. A review of the information system must be planned within a short period of time; and

  The action plan to maintain and enhance the security of the information system is acceptable.

NOTE : If the context allows, it is preferable to postpone the date of submission of the accreditation opinion in order to allow time for the teams in charge to apply new safety measures, ¬ rather than to allow its use for too short a period of time.

For information systems with excessive residual risks but which must be accredited for strategic or political reasons, a conditional accreditation opinion may be submitted.

This opinion authorises the use of the information system but requires that any actions necessary to lifting these reservations be carried out within a maximum period of 12 months.

The lifting of reservations allows the information system to maintain its accreditation beyond the defined period.

3.3.2 SIMPLIFYING AND ACCELERATING THE ACCREDITATION PROCEDURE

The following simplification mechanism may be adopted :

- **for information systems with low criticality and low exposure to digital risk sources (simplified accreditation procedure):**

  The first line of control (operational team) declares that all of the security measures which have been identified and deemed necessary to the protection of the information system, its data, and its users are applied.

  In this case, a positive security opinion may be issued by the second control line (functional team).

  Once validated by the accreditation authority, the use of the information system is authorised.

  It should be noted that a committee is not strictly required for such a case, and that a validation in electronic format is sufficient. The decision must subsequently be registered.

  Even when an information system is approved, ANSSI recommends monitoring to ensure the correct application of security

measures, in accordance with the declarations of the first control line.

If several information systems are in this case, a sample check is possible.

NOTE : The proposed sampling method consists in:
- randomly selecting information systems to be used as representative samples;
- assessing the security measures of the selected information systems and ensuring that they are understood, in line with expectations, and correctly implemented;
- extrapolating the results to all information systems.

- **for moderate-criticality or moderate-exposure systems (intermediate procedure):**
  The first control line must declare that all security measures have been applied and that all documents necessary to the accreditation of the information system in the context of an intermediate-level procedure have been provided.

  This declaration is enough to submit a positive opinion to the accreditation authority.

  The security accreditation may be granted.

  During the accreditation period, the information provided should be thoroughly analysed by the Accreditation Committee.

  If this information is in line with security expectations and challenges at hand, the accreditation is maintained.

  If that is not the case, deviations from the security requirements must be submitted to an accreditation authority as soon as possible. In this case, approval may be suspended.

For those information systems whose procedure level is simplified or intermediate, it is suggested to enhance the trust placed in the operational teams, to allow a swifter accreditation but to nevertheless a posteriori control the information transmitted.

- If these controls are successful, the accreditation process may continue and a renewal of accreditation under the same conditions may be considered.
- If these controls are inconclusive, an accreditation committee must be established as soon as possible. This committee should decide on the actions to be taken in order to ensure the information system's operational continuity.

For all other systems (reinforce procedure)

The information system's security accreditation opinion may be issued by the Accreditation Committee only after the assessment of documents justifying the consideration of security risks and the measures put in place.

The re-accreditation of information systems, whatever the level of procedure chosen, must follow the same process.

The security accreditation decision depends on the level of procedure selected:

Decision making by accreditation procedure level	Simplified	Intermediate	Reinforced
File	Self-declaration of the application of security measures	Self-declaration of the application of the security measures and the necessary information (see table "exhibits of the file to be submitted")	All of the documents within the file (see table "documents in the file to be submitted")
Submission of the accreditation opinion	CISO(second control line)	CISO(second control line)	Accreditation Committee (third control line)
Accreditation committee	May take the form of an electronic exchange	May take the form of an electronic exchange	Committee meeting (in person or remotely)

3.4. FOURTH STEP: ORGANISING THE ACCREDITATION COMMITTEE

3.4.1 PREPARING THE ACCREDITATION COMMITTEE

The Accreditation Committee congregates to present the information system to the Accreditation Authority. It is necessary for all information systems involved in a reinforced procedure.

The authority may be:

- The qualified information system security authority (AQSSI), directly responsible for the security of its own organisation's information systems. It legally responsible for their security and, in this respect, commits the organisation at the highest possible level;
- By delegation of power, the AQSSI may delegate its accreditation powers to an Accreditation Authority (AA). The AQSSI remains the legally responsible authority;
- A leader of the organisation or a manager in possession of a delegation signature from the leader. *For example, the Director of Risk.*

NOTE : To ensure an understanding of the context and a real consideration of the risks, the accreditation authority must be as close as possible to the business of the information system.

The Accreditation Committee's objective is be to decide whether an information system is to be maintained or put into service.

The Accreditation Committee should be planned sufficiently in advance. The organiser must ensure that the authority is available.

In order to ensure the smooth running of the accreditation committee, it is advisable to conduct a 'pre-committee', without the authority, to prepare the committee for any questions that may be asked. This meeting will also address residual disagreements and prepare the presentation.

3.4.2 RUNNING THE ACCREDITATION COMMITTEE

> NOTE : It is not useful to bring all of the members of the Accreditation Committee together in the committee. It is preferable to avoid overloading the meeting. However, key members of the committee must be present.

An in-person committee is strongly recommended to promote exchanges.

In the case of a remote committee, meeting equipment must be tested before the meeting and the means of videoconferencing must meet the required level of empowerment.

Ideally, the committee should not last longer than one hour, including the presentation and any questions. It is often recommended to designate a "timekeeper" in order to ensure proper time management.

Committee material must be synthetic and present the important points which are strictly necessary to the authority's decision-making.

> NOTE : The risks associated with the use of the information system must be openly and clearly exposed to the authority. They should not be undervalued or hidden.

38. For example, the evolution of the threat to the organisation or information system, struc-

The proposed duration of accreditation depends on the maturity of the information system's security, on future developments, and on its exposure to digital risk sources.

Due to the rapid evolution of threats and potential changes in IT teams, ANSSI recommends not to provide accreditations lasting longer than three years.

An information system whose action plan is substantial cannot be accredited for too long of a period.

Reducing the duration of accreditation is tantamount to increasing the monitoring of an information system.

An accreditation cannot be automatically renewed.

At the end of the accreditation period – during which the security of the information system must be improved – a new procedure must be initiated.

An accreditation which has been granted may only be reviewed at the end of its period or in the event of a significant change in the information system or its context. In this case, a new decision will need to be made upon reviewing the new accreditation documents.

It should be noted that the accreditation only pertains to the use of an information system in actual production or connected to another information system in production.

Any information system which is still being tested or designed, or which is not using real information and is disconnected from any other system in production does not require an accreditation.

Accreditation becomes mandatory before it is put into real operating condition.

> NOTE : If no reservations have been communicated at the time of pronunciation, ANSSI recommends that the accreditation decision not be reconsidered ¬before the end of the period.

Should a decision not be reached, or should an accreditation not be granted without reservations, an action plan must be drawn up and a new accreditation committee must promptly be scheduled.

The decision must be formalised in writing using the organisation's official media and communicated to the various persons concerned.

> NOTE : Informing the information system's user of its accreditation enhances trust. This can, for example, be achieved by displaying a statement upon starting the system or by communicating via one of the organisation's media.

THE ESSENTIAL :

The accreditation process must be carried out by a committee led by a manager (usually the CISO) and made up of people who are available and involved with the information system (business managers, technical experts, etc.). The committee must permit the verification of the identified risks associated with the use of the information system, and lead to the submission of an opinion to be presented to the authority.

One level of the accreditation process, out of the three proposed, must be identified. This level should correspond to the information system's criticality and exposure to risk sources.

Information proportional to the selected procedure level should be collected to compose the accreditation file.

A decision should be issued by the Accreditation Authority on the use of the information system, in view of the risks identified. This decision can be taken in a committee or via electronic communication in the context of simplified and intermediate level procedures.

The duration of the accreditation must correspond to the information system's specific security challenges, the action plan undertaken, the context of the organisation, and must not exceed three years.

To speed up and increase the number of procedures, a declaration of the application of safety measures is sufficient to issue a favourable accreditation opinion.

4

IMRPOVING THE SECURITY OF THE INFORMATION SYSTEM

The security of the information system should not end with the obtention of the accreditation. It must be maintained or improved.

This may be achieved by :

- carrying out the actions defined in the action plan, previously presented to the committee and validated by the approval authority;
- taking steps to lift any reservations made during the committee meeting;
- adding actions following any changes affecting the perimeter or ecosystem of the information system;
- maintaining the information system in operational and security condition;
- correcting identified vulnerabilities;
- applying measures pertaining to potential security incidents;
- updating the documentation.

4.1 REGULARLY REVIEWING THE SECURITY OF INFORMATION SYSTEMS

The security of an organisation's information systems must be reviewed at least once a year, without any accreditation committee.

The review should be chaired by the Accreditation Authority or by its delegate.

The duration and content of the information systems' reviewal should be adapted to the number of information systems to be studied.

During this review, the following points must be presented:

- the progress of the actions decided upon during the previous review;
- performance indicators;
- significant events, internal or external to the organisation, which may have had an impact on the security of the information systems;
- major events and security incidents during the period;
- the security-improvement efforts proposed for the following period.

It is recommended that all¬ accredited and non-accredited information systems be presented. For the latter, it is important to understand the reason for their non-accreditation.

At the end of the meeting, an appointment must be made for the next annual review.

It should be noted that any event which may affect the security of the information system – and therefore any risks associated with its use – must lead to an adaptation of the action plan and, in some cases, a a consultation with an accredidation committee.

NOTE : During the accreditation period, the accreditation authority may change. Unless specifically requested, this does not require the organisation of a new committee.

tural chances in the mainteance and improvment of the information system.

39. The procedures for destroying data and the information system must correspond to their

4.2 RENEWING A SECURITY ACCREDITATION

Prior to the end date of an information system's security accreditation, pronounced by an authority, the opinion of the authority must be renewed.

If successful, a similar procedure to the one previously implemented may be reused. Otherwise, and for any simplified and intermediate procedures, a face-to-face committee may be useful.

A properly monitored information system whose security has been improved during its accreditation period does not require major documentation efforts.

However, an accreditation committee needs to be convened to refresh the information which pertains to the information system.

It may be composed of the same persons who made up the committee during the initial accreditation.

The Committee should consider the following points :

- the 'history' of the information system, since its last accreditation: incidents, significant changes, improvements made;
- the follow-up and progress of the actions presented at the previous committee;
- contextual evolutions for the next accreditation period.

The opinion and duration proposed for the accreditation renewal may differ from the previous ones. They depend on the context and on the security issues at hand on the day of the committee..

> NOTE : It is not recommended to renew the accreditation of an information system if no actions have been taken to address its security weaknesses.

The organisation of the reaccreditation committee should be identical to that of the initial accreditation.

4.3 SHUTTING DOWN AN INFORMATION SYSTEM

The information system is considered to have been shut down when all of the data contained within it has been destroyed, declassified, transferred to another information system, or retained by a specialised service, and when all of its components have been decommissioned. Evidence must be provided for these actions.

Processes with clear instructions must be established before the decommissioning of the information system. They should be accessible and assessed by the Accreditation Committee.

Accreditation ceases when the service is withdrawn and the associated risks are removed.

THE ESSENTIAL :

Throughout its lifecycle, the security of an information system must be maintained or improved. This security should be reviewed annually at a follow-up meeting and during the accreditation phase.
Security accreditation naturally ends when the information system is decommissioned.

classification level.

THE ESSENTIAL :

Although the security accreditation procedure is a regulatory requirement for a number of information systems, it is highly recommended for the most critical information systems.

The accreditation should pertain to an information system whose perimeter has been clearly defined. All of the bricks on which it rests, its ecosystem, and the risks they entail must be identified.

The nature of the work to assess the security of the information system must correspond to its criticality and to its exposure to digital risk sources.

It is a decision taken by a competent authority, giving regard to the risks associated with the use of an information system, to the actions already taken, and to those which will be taken to reduce or eliminate these risks.

The decision is based on the opinion of the Accreditation Committee, which is responsible for collecting and assessing the actions taken to secure the information system.

An information system may be accredited even if its use involves risks which have not been addressed but which are deemed acceptable by the authority.

The duration of an accreditation depends on the security challenges at hand, the maturity of the information system, and the applicable regulations.

A security review of the information system should be carried out at least once a year.

The procedure for obtaining an accreditation is a continuation of the process to secure an information system. It must remain a simple process, useful and adapted to the information system and to its security challenges.

The information system should only be used after it has been accredited.

VOCABULARY

RISK ANALYSIS

Risk analysis (RA) is a methodological approach to identifying, assessing and addressing risks. It should lead to the creation of a risk-handling plan to reduce the likelihood of the risk occurring.

ACCREDITATION COMMITTEE

The Accreditation Committee brings together persons capable of verifying the appropriateness of the security measures applied to an information system in order to ensure that the risks to which it is exposed are acceptable.

ACCREDITATION DECISION

An accreditation decision is be taken by the accreditation authority. ¬ It grants or refuses authorisation to use an information system, in view of the risks to which it is exposed. The accreditation decision should be renewed regularly.

ACCREDITATION COMMISSION

The accreditation commission is the act through which the Accreditation Authority issues an accreditation decision. The exchanges which allow this decision may be digital (email exchanges), or they make take the form of a face-to-face meeting bringing together the persons involved in the decision.

SECURITY ACCREDITATION PROCEDURE

The accreditation process is the process which follows the life cycle of an information system. It is punctuated by accreditation phases, allowing the acceptance of risks by an accreditation authority.

EBIOS RM

EBIOS RM for the Expression of Needs and Identification of Security Risk Manager Objectives is the risk assessment method used by ANSSI and the EBIOS Club. The methodology is based on a workshop approach which builds on existing security frameworks before focusing on attack scenarios. It alternates between business and technical points of view, and aims to be effective rather than exhaustive.

REVIEW OF INFORMATION SYSTEMS

Formal point to identify the state of an organisation's information systems. The review should enable the management team to take note of the progress of the actions decided upon in previous reviews, relevant changes which might have an impact on risks, and opportunities for improvement.

SECURING AN INFORMATION SYSTEM

Process to slow down or prevent a cyberattack on an information system. The securing process is characterised by the application of governance, protection, defence, and resilience measures.

STATE INFORMATION SYSTEM

According to Decree No 2019-1088 of 25 October 2019 on the State information and communication system and the interministerial digital directorate: The information and communication system of the State is composed of the infrastructures and computer software services which allow the collection, processing, transmission, and storage in digital form of the data which contributes to the missions of the services of the State and of the bodies placed under its supervision.

REFERENCES

THE EBIOS RISK MANAGER METHOD

https://cyber.gouv.fr/la-methode-ebios-risk-manager

CARTOGRAPHY OF AN INFORMATION SYSTEM

https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation

IT HYGIENE GUIDE

https://cyber.gouv.fr/publications/guide-dhygiene-informatique

DIGITAL RISK MAINTENANCE - TRUST

https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance

PREVENTING AND MANAGING A CYBER CRISIS

https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

MY SECURE SERVICE

https://monservicesecurise.cyber.gouv.fr

CERT-FR

https://www.cert.ssi.gouv.fr

LEARN MORE

DOWNLOAD ALL TO ENSURE YOUR DIGITAL SECURITY ON THE ANSSI SITE.

More information on the ANSSI website: www.cyber.gouv.fr

Version 2.1 – April 2025
ISBN 978-2-11-167188-1 (printed) - ISBN 978-2-11-167189-8 (on line)
Legal deposit: march 2025

FRENCH CYBERSECURITY AGENCY
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr