MAPPING THE INFORMATION SYSTEM

How-to guide in 5 steps

CONTENTS

WHAT IS A MAP?

The term "map" refers to a diagram illustrating a set of information. The information shown is carefully chosen to provide an effective response to the question(s) raised.

Maps are typically organised into different dimensions. For example, geographical maps incorporate road infrastructure and towns in line with users' needs.

A varying amount of information can be displayed depending on the requirements. For example, we might choose to show altitude, service stations or toll booths on the map.

Map of the information system

In a digital context, a map provides a visual overview of an organisation's information system (IS) as well as its external connections. This overview can be more or less detailed and include, for example, the hardware assets, software, connection networks as well as the information, activities and processes which rely on these assets.

In practice, mapping must make it possible to:

- draw up the inventory of the assets of the IS, i.e. the list of its components and their detailed description;
- present the information system in the form of views, i.e. partial snapshots of the information system, its links and its operation. These aim to shed light and clarity on the different aspects of the information system.

Elements making up a map

As a general rule, the map comprises **3 visions** going progressively from business to technical aspects, themselves broken down into **views**[1]:

1. Business vision

- the **ecosystem view** presents the various entities or systems with which the IS interacts to fulfil its function;
- the **business view of the information system** shows the IS from the perspective of its main information and processes (named business assets in the risk assessment method EBIOS Risk Manager).

2. Application vision

- the **application view** describes the software components of the information system, the services they provide and the data flows between them;
- the **administration view** lists the privilege levels and scopes of users and administrators.

3. Infrastructure vision

- the **logical infrastructure view** illustrates the logical network partitioning, particularly by defining the IP address ranges, VLANs and filtering and routing functions;
- the **physical infrastructure view** describes the physical devices making up or used by the information system.

The views are made up of different objects[2], examples of which are given in Appendix 1. In each view, a pivot object shows how this view links up with the adjacent views, making it possible to identify dependencies between the objects of the information system.

1 – The division adopted here has been adjusted to the context of mapping for security purposes. It is consistent with the standards bearing on the architecture or urbanisation of information systems.

2 – The objects indicated in the appendix can meet cybersecurity purposes. It is also possible to run other projects involving mapping (such as when defining the record of processing activities pursuant to the General Data Protection Regulation (GDPR)) on the basis of this method, and to supplement it with any other relevant object.

WHY CREATE A MAP OF YOUR INFORMATION SYSTEM?

At a time when our society's digital transformation is prompting us to rethink our lifestyles and the ways we communicate, cyberattacks are growing in number and complexity. Now more than ever, cybersecurity is therefore a high-stakes issue in the smooth running of businesses and administrations.

Mapping is a key tool in keeping control over the information system. It provides insight into all of the information system's components and a clearer picture of the IS overall by presenting it from different angles, or views. Creating a map of the information system forms part of a general risk management strategy and addresses four key cybersecurity issues:

- **control of the information system:** mapping provides a shared, joint vision of the organisation's information system. It is an essential tool in managing the development of the IS over time, particularly during times of resource pooling. It also makes it easier to learn from experience and make decisions thanks to a simple, visual language. This enables the organisation's level of maturity in cybersecurity terms to be enhanced and secure conditions to be maintained;

- **protection of the information system:** by mapping the information system, the most critical and vulnerable components can be identified, the possible attack routes concerning these components anticipated and appropriate measures set up for protecting them[3];

3 – Creating a map enables a risk analysis to be conducted more easily and quickly (with the EBIOS Risk Manager methodology).

- **defence of the information system:** with a map available, the organisation can react more effectively in the event of a cyberattack or incident, qualify the impacts and anticipate the effects of the defensive measures taken;

- **resilience of the information system:** a map identifies the organisation's key activities in order to define a business continuity plan and serves as a crucial crisis management tool, whether it is digital or not.

This guide outlines an approach for helping organisations to map their information systems with a view to meeting the operational requirements of cybersecurity. It explains how to go about creating a map in simple, practical steps. It can be used by any organisation, irrespective of their type, size, maturity in terms of cybersecurity or the complexity of their information system. It has been written for organisations in the public and private sectors alike.

HOW TO CREATE A MAP OF YOUR INFORMATION SYSTEM?

Successful mapping depends on how **pragmatic, participatory and enduring** the process is. Each of the stakeholders must engage in a mapping process that is both **incremental** (enriching it by adding new views) and **iterative** (fine-tuning views that have already been created). Depending on the organisation's requirements and aims, the point is therefore to progressively map the different views and to enrich views that have already been described by adding objects, characteristics and links indicating dependency. Some details may be only partially entered to begin with, the intention being to complete them during the next iteration in keeping with the project timeline.

In order to bring the stakeholders on board, the mapping procedure must form part of the organisation's processes and the life cycle of the information system. It can be broken down into five steps, which can be tailored firstly to the type of information system being mapped and secondly to the organisation's objectives, depending on its level of maturity and cybersecurity priorities.

Step n°1

How do I get a mapping project up and running?

Define the key issues, which stakeholders to get involved, the scope of the information system to be depicted, the level of detail required in the inventory, the types of view to be captured, the different iterations and the associated timeline.

Step n°2

Which model should I adopt?

List all of the information available by gathering together existing inventories and diagrams bearing on the information system. Define the model for compiling the inventory and the different views as well as a nomenclature for the different objects.

Step n°3

Which tools should I use?

Identify the necessary tools for creating the map and keeping it up-to-date.

Step n°4

How do I create my map step-by-step?

Compile the inventory by updating, where applicable, the information listed and completing it in keeping with the model defined. Lay out the different views of the map according to the model.

Step n°5

How do I ensure my map remains relevant over time?

Circulate and promote the map within the organisation. Set up a process and the associated governance[10] for updating the map. ●

4 – In this context, by governance we mean identify the roles and responsibilities of each stakeholder in sustaining the map and the committee procedure behind the management and monitoring of its updating.

Step n°

1

HOW DO I GET A MAPPING PROJECT UP AND RUNNING?

In this first step, you are going to define, together with all of the stakeholders, all the elements necessary for getting the mapping project up and running smoothly.

1 Identify the key issues and stakeholders involved in creating the map

You need to begin by **clearly defining the aims and issues shaping the mapping project** so as to meet the organisation's needs.

The aims of the mapping project must be shared by all of the stakeholders and validated by a sponsor. The project's sponsor shall be a **member of the organisation's management board** and play an active part in the governance of the mapping project.

Where the process for mapping the information system is geared towards cybersecurity, the number of stakeholders involved will be limited. The **cybersecurity manager** must act as the coordinator and take on responsibility for setting up and monitoring the process.

Where the organisation is keen to embark on a more general, comprehensive mapping of its information system, incorporating the cybersecurity requirements, the **CIO**[5] could oversee the project. S/he would coordinate a team made up of a large number of stakeholders, whose roles and responsibilities must be clearly defined – this is essential. Potential stakeholders in the mapping project include the cybersecurity manager, architects, business specialists, the DPO[6], safety managers or audit and compliance teams for example. The departments will have to assist with and support the setup of this team.

5 – Chief information officer.
6 – Data protection officer.

Note

It is essential that the IT and cybersecurity teams work together so that the map created covers both teams' requirements – particularly if the cybersecurity manager is not positioned within the IT department. It will not be possible to keep a map geared solely towards cybersecurity relevant as the information system is upgraded over time. Likewise, a map focusing solely on the information system will not be appropriate for cybersecurity use.

The map must not be the sole responsibility of the IT and cybersecurity teams alone. It must also involve the business specialists, as owners of their processes and data. By getting the stakeholders involved in this way, the map will be adopted more easily. For example, it could serve as a useful tool for providing them with an overview of the stakeholders in their ecosystem.

2 Define the scope to be mapped

What needs doing next is to **formally define the scope to be mapped** so as to make sure all of the parties involved in the process share the same vision.

Whatever the aims set, it is recommended **to begin by mapping the most exposed or the most critical systems** (for operations, for the company's finances, for the Nation). These systems are the most sensitive regarding their security requirements and the most vulnerable in terms of exposure to threats.

3 Define the mapping target and the construction path

Defining the **target** entails **identifying all of the views** to be created as well as their **level of detail**. The detail of the map's views is to be tailored to the context and the aims in mind. It can therefore vary from one information system to another, depending on its criticality or the importance attached to it.

By drawing up a **construction path** you can **plan the different iterations and key milestones** in the mapping process. Adopting a progressive timeline is recommended, based on the gradual achievement of increasing levels of maturity, i.e. in phases.

Defining the target and timeline allows you to **determine the responsibilities of the different stakeholders, estimate the resources to set aside and define the schedule**. One method for creating the map in keeping with the different stages of maturity is described in Appendix 2.

For a large information system, it is recommended to begin with a map that is limited to certain views and focused on the critical or exposed systems, which will then be expanded by adding more views at a subsequent stage.

For a small IS, it is possible to create a map that brings together several views from the outset. ●

Step n°

2

WHICH MODEL SHOULD I ADOPT?

During step two, you will gather all of the inventories and diagrams illustrating the information system that have already been compiled. Then, you will define the model for presenting the inventory and the different views. In practice, the model is defined at the same time as collection so that it is adjusted in line with the feedback obtained.

1 Collect and analyse the existing mapping elements

By analysing what already exists, you can speed up the mapping process as in this way you can **gather together all of the work that has already been carried out** and thus form a starting point.

Holding **interviews** with the organisation's stakeholders involved in cybersecurity, design and operation of the information system is an opportunity **to present the mapping process, gather existing information and identify the first gaps** (with regard to the mapping model defined at the same time).

We would recommend paying particular attention to the following tasks:

- gathering and analysing all of the documents bearing on the description of the information system, the standards used and the inventory of resources and assets;
- identifying any mapping tools already in place;
- identifying the existing processes concerning the provision and updating of asset information;
- identifying the difficulties encountered in compiling and using previous maps.

2 Define the mapping model

By defining a mapping model, the organisation obtains a **common framework** that will ensure successful communication and sharing of information between all of the organisation's stakeholders. The contents of the model will vary depending on the views to be developed – chosen in Step 1.

For each of the map's views, it is necessary to **choose the objects and attributes** to be shown as well as their graphic representation. The **objects** are a set of elements referenced in the map – which correspond to the **business and supporting assets** in the meaning of the EBIOS Risk Manager methodology. The relationships between objects can also be shown (pivot objects present in different views, significance of the dependency between objects, etc.). Lists of objects are presented for each view in Appendix 1. These contain not only the objects that are usually encountered in urbanisation models, but also the objects that specifically address the requirements of cybersecurity. The **attributes** are key pieces of information for future analyses, some of which have to do with cybersecurity. For example, it is possible to distinguish for an application **its type** (internal development, software, software package, etc.), **its security requirements or its external exposure**. The mapping model should define the list of attributes corresponding to each chosen object, with a priority for those associated with cybersecurity. Lists of attributes are presented for each object in Appendix 1.

Finally, the definition of the mapping model also includes the definition of the **expected graphic representation** for each object and attribute, as well as compliance with a **nomenclature** making it possible to have uniform information to hand. The function of the objects and attributes must be clearly conveyed in their illustration so as to facilitate their use and movement from one view to another (e.g. same shapes, colours, nomenclature, etc.). ●

Step n°

3

WHICH TOOLS SHOULD I USE?

In this third step, you are going to define the software tool(s) you will be using to bring your mapping project to a successful conclusion. The choice of more or less specialised tools depends on the target level of maturity and the context.

Using **specific software** (software for modelling the information system or enterprise architecture software) swiftly becomes essential when the volume of data and/or number of contributors becomes considerable.

The tools chosen must meet the following requirements[7]:

- compiling the inventory;
- creating views and showing the links between them;
- implementing and supervising the processes for keeping the map up-to-date.

It is quite possible that the tools concerning inventory, management of physical movements or infrastructure modelling are already set up in the organisation or that certain systems propose maps on certain parameters. The aim of the mapping project is not to replace existing tools. However, it is important **to check that the tools in place still correspond to current use, and to identify to what extent they may be useful in carrying out the mapping project**. Should the tools in place no longer be appropriate, the choice of a new tool may be proposed.

Note

The tool's simplicity is a major advantage in delivering an effective mapping project and avoids the creation or discovery of "parallel" maps.

7 – The tools may also be used to cater for additional requirements such as the association of documentation with the map's objects, graphic display of dependencies between objects, creation of relationships between objects and their owners, creation of maps depending on the model of the organisation (by department, by subsidiary, by country, etc.), etc.

In addition to their usefulness in producing diagrams and inventories, **tools for modelling the information system** also help to **simplify updates and information sharing**. For example, some automatically incorporate any changes as they happen into the views in the inventory (and vice versa) so as to guarantee overall consistency and interdependencies between the components of the IS. The process automation features available in some software can be used to carry out validation stages and reminders among the stakeholders responsible for updates in a particular area.

There are few software options out there for collecting information directly. That said the most flexible can **interface with data collection tools** (systems management tool, IP address management, etc.).

Accordingly, tools for modelling the information system make such collection easier and thus prove to be great time-savers. They guarantee consistency in terms of content and depiction of the systems, both as regards substance and form, and clarify them for readers. The maps are also centralised within a single framework, with easy access for the stakeholders involved.

In all cases, and for successful sharing of information, it is strongly recommended that the map could be exported in a format that can be read by the main office software, in read-only mode. ●

Step n°

4

HOW DO I CREATE MY MAP STEP-BY-STEP?

In step four, you will draw up the inventory and create the mapping views using the tool(s) that will have been chosen during the previous step and according to the timeline defined during step one.

A successful mapping project particularly depends on the process being a progressive one. The inventory and the different views should be created in stages, in a manner that is:

- **incremental** (enriching it by adding new views);
- **iterative** (fine-tuning views that have already been created).

Particular attention should be paid to the **sensitivity of the information** contained in the inventory and the views of the map. If justified by the protection requirement, the project manager or cybersecurity manager may decide to specify a protection indication on the map (Business Confidential or even a level of classification).

1 Draw up the inventory of the information system

The **inventory of the information system** is drawn up on the basis of the information gathered during the analysis of what already exists. The aim here is to round off this information with the information defined in the model, during step 2.

To compile an exhaustive inventory of the elements making up a view, it is, for example, possible to explore the elements gradually **by taking a list of objects as your starting point and by following the dependency links**.

You can also complete the inventory through:

- targeted interviews planned on the basis of information that was collected during the analysis of what already exists;
- automated collection tools as systems management tools or supervision software;
- data sets extracted from specific applications (databases, dashboards, etc.);
- internal documents, such as business continuity and recovery plans or risk analyses.

2 Create the mapping views

Not all of the objects and attributes of the inventory are necessarily meant to be shown on the mapping views: the views can have different levels of detail.

That being so, **it is important that the links between the pivot objects are exhaustive** for the cybersecurity impacts assessment. These diagrams are typically the first elements to be examined during post-incident analyses or audits, as they provide a quick insight into the information system.

The mapping views are generated by dedicated tools. It is important **to consider each diagram as a snapshot at a particular point in time**, rather than as a definitive diagram or final picture. Should a view that has not been defined by the tools prove necessary, creating this manually from extractions is not recommended. Most tools feature complementary modules or extensions – this is the better option.

Note

Each diagram should contain a title, a date, a version number and a caption.

To depict all of the elements making up each view, as when drawing up the inventory, a step-by-step process is possible. An added element is thus immediately connected to the elements that are already shown. Remember that the different elements must be presented according to the format defined during step 2. ●

Step n°

5

HOW DO I ENSURE MY MAP REMAINS RELEVANT OVER TIME?

The four previous steps will have enabled an initial picture of the organisation's assets to be gained. But a map is only of use if it is communicated as widely as possible and if the information it contains is reliable and up-to-date. This means that to retain its value and relevance over time, the map must be shared and reviewed at regular intervals. This is the point of step five.

1 Communicate about the map

For maximum effectiveness, **communication must form an integral part of the map updating process**. It is nevertheless essential to take on board the sensitivity or confidential nature of certain information, and limiting access to the different mapping views is therefore recommended – so that only the relevant persons can access them. Infrastructure views, for instance, will only be accessible to the CIO team, whereas the business view may be shared more widely. The map must particularly be made available to the cybersecurity manager and CERT[8] of the organisation (or equivalent setup).

8 – Computer emergency response team.

Note

The map of the information system represents a key element of the organisation. As such, measures must be taken to guarantee its availability and confidentiality:

- *the map must be saved at regular intervals on a secure storage medium. It must particularly be accessible in the event of network failure. Keeping a paper version of it, as up-to-date as possible, is one solution in this regard. Such a version shall have to be secured according to the map's classification level.*
- *the map should not be stored on the information system it depicts. Otherwise, an adversary who has managed to break into the IS would then have access to all the information concerning the system's architecture. In addition, access to the map should be limited on a need-to-know basis (i.e. to the business specialists for the views concerning them, the IT department, or the members of the crisis unit for example), so as to reduce the risk of leaks.*

2 Keep the map up-to-date

Whatever the size or type of organisation, it needs to have sufficient resources to **keep the map up-to-date.** These resources will depend on the level of maturity reached. Making sure there is a specific role assigned to supervising updates, noting down the model's upgrading requirements and assisting the teams who are involved in the mapping project is crucial.

Measures aimed at reviewing the map must be organised via a **continual improvement process and governance that have been clearly defined**, so as to avoid a situation where there are multiple versions for example. One good practice could be to **set up regular updating campaigns** that require

input from the stakeholders concerned, by checking and updating the information in their perimeter.

In the context of a map's review, the stakeholders could answer the following questions:

- Does the scope of the map need to be extended?
- Should we be aiming for a higher maturity level?
- Do some of the views already depicted need fine-tuning?
- What is the preferred timeframe for completing the next tasks?

Another good practice is to **incorporate a map updating stage** into information system upgrading projects.

KEY SUCCESS FACTORS

Mapping can turn out to be quite a complex process, with organisational, human, technical or timing problems cropping up along the way. The advice set out in this section will help you to achieve the results you are after more easily.

Track a project process and keep its outcome relevant over time

Underpinning a mapping process should be a development strategy which sets realistic targets and priorities in terms of content and schedule, is rolled out in project mode and involves the highest levels of the organisation's management. To help keep the map relevant over time, give precedence to up-to-date macroscopic information as opposed to detailed information which is only updated sporadically at unnecessarily great expense.

Create the map in iterations

Mapping the whole of an information system in the short term, covering all of the worthwhile information and associated views, is often very difficult – if not impossible. The map should form part of a continual improvement strategy that is both incremental and iterative. This strategy enables the map's coverage to be broadened, level of maturity to be increased and the processes underway to be increasingly improved and optimised so as to meet the new cybersecurity requirements.

Adopt a mapping model as a common language

To make it easier to share information, the stakeholders should rely on a common language. The mapping model's definition is a decisive stage in the process, when concepts shared between the different actors can be established. It is essential that these concepts are clearly defined and tailored to the context of use and, as such, these definitions must have been unambiguously and tangibly grasped by each stakeholder.

Communicate at every stage of the project

Communication during a mapping project matters, irrespective of what stage the process has reached. It is particularly important to communicate about the process at the project outset, by highlighting its usefulness and aims (for example, significant improvement in the control of the information system, responsiveness in the event of failure, management of system upgrades, etc.). Such communication must make it possible to unite the actors around the process. Once this is complete, it is also essential that the map is made available to the teams for whom it may serve a purpose (depending on its level of confidentiality).

Keep the map up-to-date

Updating the map is also a key stage in the process so as to guarantee that developments to the information system are conveyed in the inventory and views as they unfold. The choice of tool is crucial so as to simplify the tasks of creating and updating the map. It is also necessary to define and set up a process for updating the map and its associated governance. The map must be reviewed in a regular and structured manner. ●

APPENDICES

APPENDIX 1
DEFINITION AND SUGGESTION OF CONTENT FOR THE DIFFERENT VIEWS

This appendix **defines the different views presented during Step 1** and suggests content ideas for each one. We recommend **selecting the elements to be listed from among these suggestions**, and **possibly completing them** depending on the organisation's requirements and context. The elements proposed for the different views are not necessarily all meant to be shown in the diagrams.

Each element has its corresponding level of detail. Three ascending levels are listed in this guide:

- **1 - minimum level of detail:** essential information;
- **2 - medium level of detail:** key information;
- **3 - in-depth level of detail:** useful information.

The objects and attributes mentioned in the various tables of this appendix, along with the associated levels of detail, are suggestions that tie in consistently with the timeline proposed in Appendix 2. When defining its mapping target and timeline, each organisation is free to define new objects or attributes and to adapt each element's level of detail as required.

Note

The attributes mentioned in blue are geared towards cybersecurity.

1 Ecosystem view

The ecosystem view describes **all of the entities or systems that gravitate around the information system** for which the mapping is being carried out. This view makes it possible to define the **scope of the mapping** and to obtain an **overview of the ecosystem**, without making do solely with an individual study of each entity.

Object	Attribute	Level of detail	Pivot object
Entity or system	Identification and description	1	
	Type of entity or system (e.g. internal, external, provider, customer)		
	Security level (e.g. maturity, security measures in place or defined contractually, degree of trust, accreditation)		
	List of processes supported		View 2
	Entity's security point of contact (e.g. cybersecurity manager)		
Relationship	Type (e.g. provision of goods, services, sales partnership)	1	
	Contractual or statutory link	2	
	Relationship's level of functional importance		

2 Business view of the information system

The business view of the information system describes **all of the organisation's business processes with the stakeholders involved**, regardless of the technological choices made by the organisation and the resources placed at its disposal. The business view is crucial as it enables **the technical elements to be repositioned in their business environment and thus for their context of use to be understood**.

A process is described from start to finish, from the trigger event right through to the final outcome, regardless of any partitioning existing within the organisation. For cross-cutting processes under the governance of several entities,

a structure must be planned to describe them in their entirety – retaining a perception shared by all of the stakeholders.

This view also displays the organisation's information – some of which may be critical and represent preferred targets during attacks.

Object	Attribute	Level of detail	Pivot object
Macro process	Identification and description	2	
	Incoming and outgoing elements		
	List of constituent processes		
	Security requirements (CIAT)		
	Owner	3	
Process	Identification and description	1	
	Incoming and outgoing elements		
	List of constituent activities (or constituent operations where maturity levels 1 or 2[9] are targeted)		
	List of associated systems of entities		View 1
	List of supporting applications		View 3
	Security requirements (CIAT)		
	Owner		
Activity	Identification and description	3	
	List of constituent operations		
Operation	Identification and description	1	
	List of constituent tasks	3	
	List of stakeholders involved	2	
Task	Identification and description	3	
Stakeholder	Name and contact information	2	
	Type: person, group, entity, etc.		
	Type: internal or external to the organisation		

9 – As defined in Appendix 2.

Object	Attribute	Level of detail	Pivot object
Information	Identification and description	1	
	Owner		
	Administrator		
	Storage (type, location)		
	Associated process		
	Security requirements (CIAT)		
	Sensitivity: personal data, medical data, classified data, etc.		
	Regulatory and standards-related requirements	3	

3 Application view

The application view is an opportunity to describe part of what is traditionally referred to as the IT system. This view describes **the technological solutions supporting the business processes** – primarily the applications.

From a cybersecurity point of view, application flows are considered to be of major importance. This view is particularly useful for viewing information exchanges from a software perspective. The exchange arrangements are characterised here in detail.

Object	Attribute	Level of detail	Pivot object
Application unit	Identification and description	2	
	Manager		
	List of constituent applications		
Application	Identification and description	1	
	List of using entity(ies)	2	View 1
	Entity responsible for operations		
	Cybersecurity manager	1	
	Type of technology: thick-client, Web, etc.		

Object	Attribute	Level of detail	Pivot object
Application	Type of application: internal development, software, software package, script, EAI/ESB platform, etc.	1	
	Volume of users and profiles	2	
	Associated flows	1	
	Security requirements (CIAT)		
	External exposure (e.g. Software as a Service – SaaS type solution)		
	List of processes using the application		View 2
	List of application services delivered by the application	2	
	List of databases used by the application	1	
	List of logical servers supporting the application		View 5
Application service	Identification and description	2	
	List of constituent modules		
	Associated flows		
	External exposure (e.g. Cloud service)		
Module	Identification and description	2	
	Associated flows		
Database	Identification and description	1	
	List of using entity(ies)	2	View 1
	Entity responsible for operations		
	Cybersecurity manager	1	
	Type of technology		
	Associated flows		
	List of information contained		View 1
	Security requirements (CIAT)		
	External exposure		
Flows	Identification and description	1	
	Emitter: application, module, database, etc.		
	Receiver: application, module, database, etc.		
	Encryption		

4 Administration view

The administration view is a special case of the application view. It lists the **privilege levels and scopes of administrators**.

The diagram setting out this view is only of use in the case of centralised management of administration access rights to devices comprising several administration scopes. Where the access rights to devices are managed by local accounts, it is reduced to a list of accounts and associated rights for each device.

Object	Attribute	Level of detail
Zone of administration	Identification and description	1
	Group of administrators and privilege levels	
	List of elements contained in the zone	
	List of secrets associated with the administration of resources	
Administration directory service	Identification and description	1
	Solution: Active Directory, Novell, NT4, Samba, etc.	
Active Directory Forest / LDAP Tree Structure	Identification and description	1
	Domains belonging to the forest/tree structure	
	Inter-forest/inter-tree relationships: domains, two-way, filtered, transitive, etc.	
Active Directory / LDAP Domain	Identification and description	1
	Number of domain controllers	
	Number of user accounts attached	
	Number of machines attached	
	Inter-domain relationships: domains, two-way, filtered, etc.	

5 Logical infrastructure view

This view corresponds to the **logical distribution of the network**. It illustrates **the partitioning of networks and logical links between them.** Moreover, it lists the network devices in charge of traffic.

The logical locations of security devices (sensor, firewall, SIEM, etc.) are also listed in this view.

Object	Attribute	Level of detail	Pivot object
Network	Identification and description	1	
	Type of protocol		
	Operations manager		
	Cybersecurity manager		
	Sub-networks attached		
	Level of sensitivity or classification		
Sub-network	Identification and description	1	
	Address/Mask		
	Gateway		
	IP address range: start and end address		
	IP assignment method: static or dynamic		
	Operations manager		
	DMZ or not		
	List of interconnected sub-networks		
	Possibility of wireless access		
Entry gateway from the outside	Technical characteristics	1	
	Public and private IP address		
	Type of authentication		
Connected external entity	Name, Cybersecurity Manager, IS contacts	2	
	Internal networks interconnected to the entity		

Object	Attribute	Level of detail	Pivot object
Switch	Identification: IP address and identifier	1	
	Technical characteristics: model, embedded software version		
	Network flow filtering rules	2	
	Physical support device (if virtualised)		View 6
Router	Identification: IP address and identifier	1	
	Technical characteristics: model, embedded software version		
	Network flow filtering rules	2	
	Physical support device (if virtualised)		View 6
Security device	Identification (identifier, IP address, MAC address) and description	1	
	Technical characteristics: type of device (sensor, firewall, SIEM, etc.), model, OS and version, embedded software version		
	Physical support device (if virtualised)	2	View 6
DHCP server	Identification (identifier, IP address if static, MAC address) and description	2	
	Technical characteristics: model, OS and version		
	Physical support server (if virtual machine)		View 6
DNS server	Identification (identifier, IP address if static, MAC address) and description	2	
	Technical characteristics: model, OS and version		
	Physical support server (if virtual machine)		View 6
Logical server	Identification (identifier, IP address, MAC address) and description	1	
	Technical characteristics: model, OS and version		
	Active network services		
	Physical support server	2	View 6
	Linked applications	1	View 3

6 Physical infrastructure view

The physical infrastructure view **describes the physical devices** making up or used by the information system. This view corresponds to the **geographic distribution of network devices within the different sites of the organisation**. It provides an overview of the assets connected to the company's telecommunication network.

Object	Attribute	Level of detail	Pivot object
Site	Identification and description	1	
	Buildings attached		
Building/Room	Identification and description	1	
	Bays attached		
Bay	Identification and description	1	
	List of hosted machines		
Physical server	Identification: identifier, IP address, DNS name	1	
	Technical characteristics: type, model, OS and version		
	Physical location: site, building, room, bay		
	Logical server(s) attached		View 5
	List of connected switches		
	Operations Manager		
Workstation	Identification	2	
	Technical characteristics: type (desktops or laptops), model, OS and version		
	Physical location: site, building, room		
Storage infrastructure	Identification	2	
	Technical characteristics: type (NAS, SAN, hard drive, etc.), model		
	Physical location: site, building, room, bay		

Object	Attribute	Level of detail	Pivot object
Peripheral	Identification	2	
	Technical characteristics: type (printer, scanner, etc.), model		
	Operations Manager		
Telephone	Identification	2	
	Technical characteristics: type (desktop or laptop), model		
	Physical location: site, building, room		
Physical switch	Identification	1	
	Logical switch(es) attached		View 5
	Technical characteristics: level (L1, L2, L3, etc.), model, embedded software version		
	Physical location: site, building, room, bay		
	VLAN associated		
Physical router	Identification	1	
	Logical router associated		View 5
	Technical characteristics: model, embedded software version		
	Physical location: site, building, room, bay		
	VLAN associated		
Wi-Fi terminal	Identification	2	
	Technical characteristics: model		
	Physical location: site, building, room, bay		
Physical security device	Identification (identifier, IP address, MAC address) and description	1	
	Logical security device(s) attached		View 5
	Technical characteristics: type of device (sensor, firewall, SIEM, etc.), model, OS and version, embedded software version		
	Physical location: site, building, room		
WAN	Identification	1	
	MAN or LAN attached		

Object	Attribute	Level of detail	Pivot object
MAN	Identification	1	
	LAN attached		
LAN	Identification	1	
VLAN	Identification and description	1	
	Switches associated		

APPENDIX 2
PROPOSAL OF A MAPPING TARGET AND CONSTRUCTION PATH

This appendix proposes **an example of target and construction path for creating a map as and when the maturity levels are reached**.

When defining the mapping aims, it is possible to either lean towards an approach centred on cybersecurity, overseen by the cybersecurity manager, or a more general approach overseen by the CIO, meeting all of the mapping requirements. The requirements of the mapping project must be validated by a sponsor – a member of the organisation's management board.

The target maturity level is then defined in keeping with the choice of project approach:

- **maturity level 1:** the approach sets out to create a map consisting of the **core elements essential** to cybersecurity operations. This level is regarded as an **intermediate stage**, centred on a limited number of views, and intended to gradually work its way up to maturity level 2;
- **maturity level 2:** the approach sets out to create a map geared towards cybersecurity in which **all of the views are shown**;
- **maturity level 3:** the approach sets out to create an **exhaustive and detailed map which incorporates the requirements of cybersecurity**. The level of detail of the different views is more in-depth so as to obtain a complete picture of the information system.

The table below presents the information collected for each maturity level.

Objects/Attributes involved	Mapping approach geared towards cybersecurity		General mapping approach
	Maturity level 1	Maturity level 2	Maturity level 3
Ecosystem view			
Level of detail 1	●	●	●
Level of detail 2			●
Business view of the system			
Level of detail 1	●	●	●
Level of detail 2		●	●
Level of detail 3			●
Application view			
Level of detail 1	●	●	●
Level of detail 2			●
Administration view			
Level of detail 1		●	●
Logical infrastructure view			
Level of detail 1	●	●	●
Level of detail 2		●	●
Physical infrastructure view			
Level of detail 1		●	●
Level of detail 2			●

APPENDIX 3
MAPPING EXAMPLE

This appendix provides an example of application based on a case study on a road tunnel carried out by **ANSSI**[10].

The maturity level of the mapping of this practical case is 1, and it is organised around three views with a level of detail of 1: a business view, an application view and a technical architecture view. The business view of the ecosystem is not shown since only the tunnelling machine is present in the ecosystem.

The mapping example concerns the industrial information system of a fictitious road tunnel located under Mont Aigoual, on the road linking Meyrueis with Notre-Dame-de-la-Rouvière.

Figure 1 – Location map

This a road tunnel of the bidirectional single-tube, with a length of 2,550 m. The tunnel is supervised from a main remote control centre, located in Millau. It also has a secondary control centre, used as a backup, located on-site on the Meyrueis side.

10 – *Agence nationale de la sécurité des systèmes d'information.* The French version of the case study is available on ANSSI website – https://www.ssi.gouv.fr/

Inside the tunnel, technical rooms (recesses) are installed about every 200 m. There are also tapping points for the various fluids, electrical power supplies or switches for the IT networks.

The missions of the tunnel are as follows:

- allow for the transit of vehicles from the entrance to the exit of the tunnel;
- ensure the safety of users and staff during nominal operation;
- ensure the safety of users and staff in case of fire or the presence of gas.

In order to ensure a satisfactory level of operating safety in the tunnel, the functions are as follows:

- electrical power supply and distribution;
- indication of emergency exits;
- ventilation;
- signalling;
- detection of oversize vehicles;
- video surveillance;
- fire detection;
- emergency call network;
- air quality control;
- acquisition and processing of data from the tunnel (remote measurements, remote alarms, remote signalling): supervision;
- control of devices by sending controls and settings remotely: monitoring.

According to the method formally set out in the guide *Cybersecurity for Industrial Control Systems*[11], a classification of the key functions has been defined in light of the likelihood and impact of an attack on each function. For industrial systems, the method documented in the guide puts forward 3 classes

11 – French version of the document available on ANSSI website.

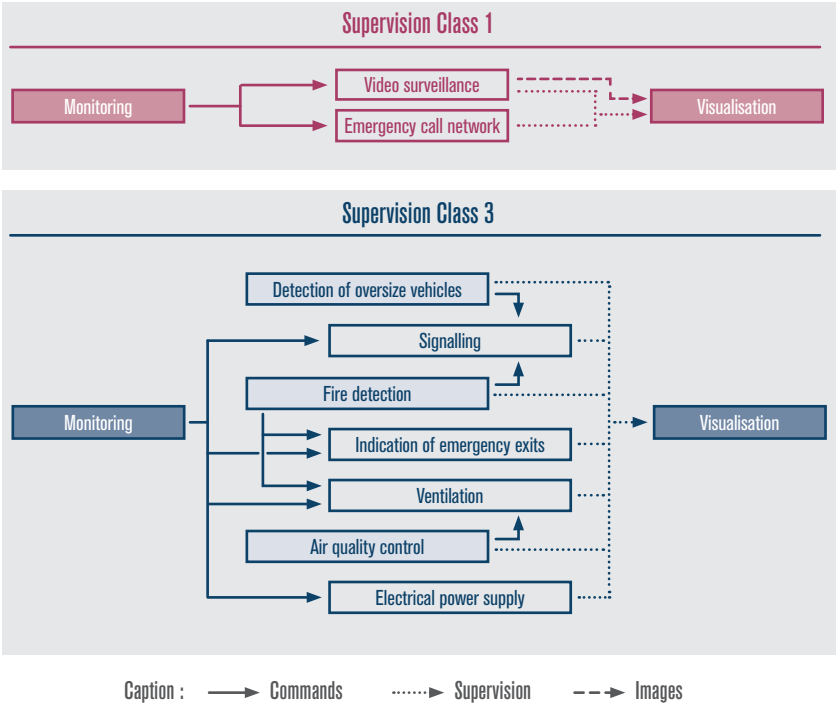
numbered 1 to 3, in ascending order of criticality and which are defined as follows:

- **class 1:** the risk and impact of an attack are low;
- **class 2:** the risk or impact of an attack is significant;
- **class 3:** the risk or impact of an attack is critical.

In order to limit the restrictions on class 2 devices whilst reducing the technical and operational complexity of the whole, the decision was made to group class 2 elements together with class 3 elements.

The outcome of the analysis is illustrated by the business view, shown in Figure 2.

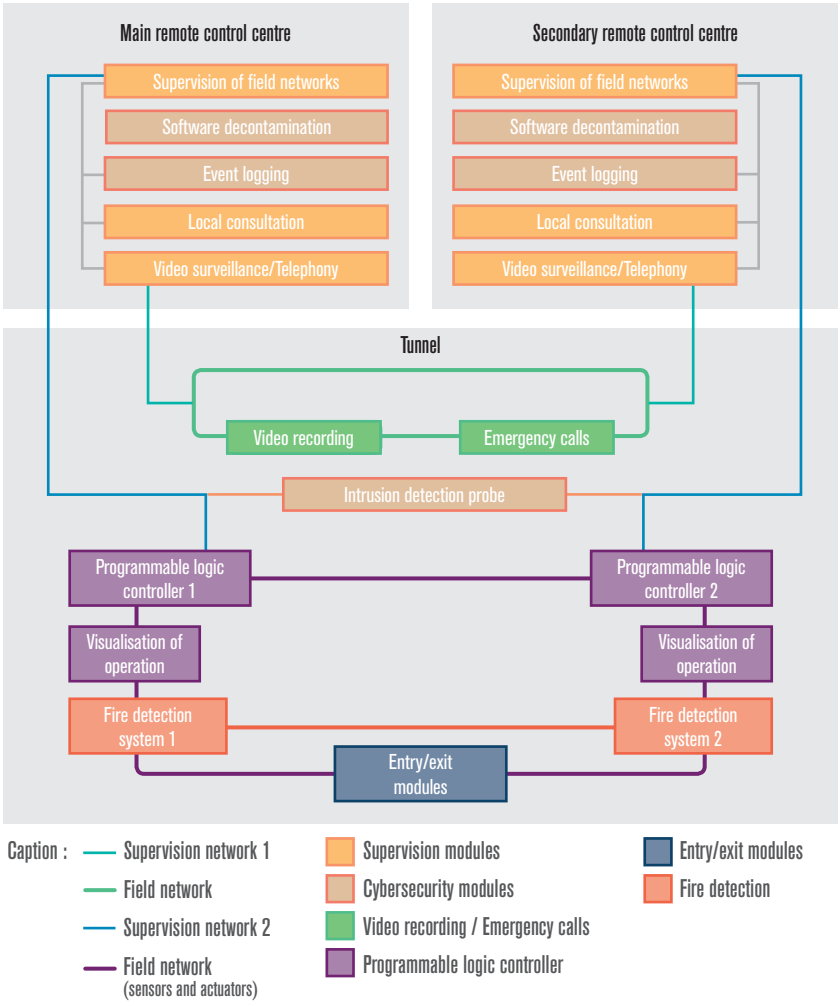
Figure 2 – Business view of the information system



From this analysis and the resulting business organisation, a more complete presentation has been carried out of all of the key measures described in *Cybersecurity for Industrial Control Systems*, from which the architecture diagrams have been taken.

The application view displayed in Figure 3 shows the different application modules which contribute to keeping the industrial system secure.

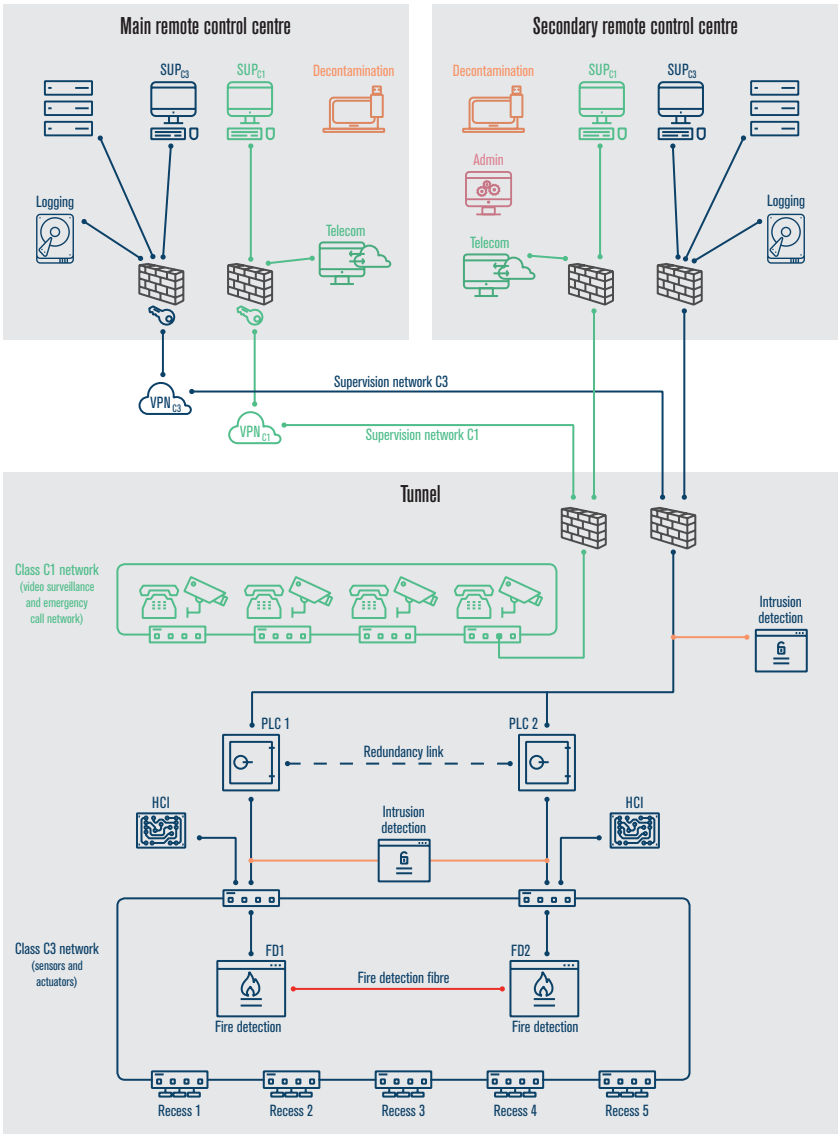
Figure 3 – Application view of the information system



The view of the information system's technical architecture is shown in Figure 4.

In this view you can see that the class 1 and 3 field networks are not connected. The devices which are connected to them are managed from a dedicated supervision workstation. On each site, there is also a decontamination workstation that is not connected to any network. At the tunnel entrance on the secondary site, an administration station is placed in a cabinet. It is dedicated to interventions on devices that can only be administered locally.

Figure 4 – Technical infrastructure view of the information system



APPENDIX 4
GLOSSARY

Active Directory / LDAP Domain	Set of elements (members, resources) governed by the same security policy.
Active Directory Forest / LDAP Tree Structure	Organised group of Active Directory / LDAP domains.
Activity	Key stage in the implementation of a process. It corresponds to specific expertise and not necessarily to an organisational structure of the company.
Administration directory service	Application grouping together data about the company's IT devices or users and enabling their administration.
Application	Consistent set of IT objects (executables, programs, data, etc.). This is a group of application services.
Application service	Component of the application made available to the end user as part of his/her work. An application service may, for example, be a Cloud service.
Application unit	Set of applications.
Bay	Technical cabinet containing the telephone or IT network devices.
Building/Room	Location of people or resources inside a site.
CIAT	Security requirements: Confidentiality, Integrity, Availability, Traceability.
Database	Structured and organised set of information intended for computer use.
DHCP server	Physical or virtual device for managing a network's IP addresses.
DMZ	Demilitarised zone – Network zone that is isolated both from the internal network and external network, containing the services that can be accessed from the outside.
DNS server	Domain Name System – Physical or virtual device for converting a domain name to an IP address.
Entity or system	Part of the organisation (e.g. subsidiary, department, etc.) or information system in relation with the IS which is to be mapped.
Entry gateway from the outside	Component connecting a local network with the outside.
Flows	Exchange of information between a transmitter and receiver (application service, application or stakeholder).
Information	Piece of data subject to computer processing.

LAN	Local area network: computer network that interconnects devices within a limited area.
Logical server	Logical division of a physical server.
Macro process	Set of processes.
MAN	Metropolitan area network: computer network that interconnects devices over medium distances. It typically interconnects different LANs.
Module	Component of an application characterised by functional consistency in computer terms and technological uniformity.
Network	Set of logically interconnected devices which exchange information.
Operation	Stage in a procedure corresponding to a stakeholder's involvement in an activity.
Peripheral	Physical component connected to a workstation for adding new accessories (e.g.: keyboard, mouse, printer, scanner, etc.).
Physical server	Physical machine performing a set of computer services.
Process	Set of activities contributing to an objective. The process generates information (output) with added value (in the form of deliverables) using information (input) generated by other processes.
Relationship	Link between two entities or systems.
Router	Component managing the connections between different networks.
Security device	Component enabling supervision of the network, detection of incidents, protection of devices or which keeps the information system secure.
SIEM	Security Information and Event Management – log correlation and management tool.
Site	Geographic location bringing together a group of people and/or resources.
Stakeholder	Representative of a business role, who performs operations, uses applications and makes decisions with regard to processes. This role may be carried out by a person, a group of people or an entity.
Storage infrastructure	Physical medium or network for storing data: network-attached storage (NAS), storage area network (SAN), hard drive, etc.
Sub-network	Logical subdivision of a larger network.
Switch	Component managing the connections between the different servers within a network.

Task	Elementary activity carried out by an organisational function and forming an indivisible work unit in a process value chain.
Telephone	Landline or mobile belonging to the organisation.
Urbanisation	The urbanisation of information systems entails processing and aligning an organisation's assets (information and communication technology, staff, projects, processes) with its own operational characteristics, development strategy and limitations, all within a formal, clear and shared framework
VLAN	Virtual local area network (LAN) enabling the logical grouping together of devices by overcoming physical restrictions.
WAN	Wide Area Network: computer network that interconnects devices over long distances. It typically interconnects MANs or LANs.
Wi-Fi terminal	Hardware enabling access to the Wi-Fi wireless network.
Workstation	Physical machine enabling a user to access the information system.
Zone of administration	Set of resources (people, data, devices), under the responsibility of one (or more) administrator(s).

Version 1.0 - November 2018
ANSSI-PA-046

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
www.ssi.gouv.fr/ communication@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre