FOSDEM'23

Mercator

Mapping the
Information System

February, 4th 2023

Mercator

Mercator?

Mercator is a web application that allows you to manage the mapping of an information system as described in the Information System Mapping Guide from ANSSI.fr

What is a mapping ?

Mapping is a way to represent the information system of an organization as well as its connections with the outside world. The term "mapping" refers to a schematic representation of a set of information.

Mapping <-> Inventory

Who is Mercator?

Mercator is a cartographer. He is the author of the Mercator projection, which is a conformal projection, i.e. it keeps the angles (very useful in sailing in the 16th century).

Mercator

Why map?

Essential tool to control the information system. It allows you to have knowledge of all the components of the information system and to obtain a better understanding of it by presenting it under different views.

Four challenges of digital security

The control of the information system: the cartography allows to have a common and shared vision of the information system within the organization.

Protection of the information system: mapping makes it possible to identify the most critical and most exposed systems, to anticipate possible attack paths on these systems and to implement adequate measures to ensure their protection.

Defense of the information system: mapping enables a more effective response in the event of an incident or digital attack, to qualify the impacts and predict the consequences of the defensive actions taken

Information system resilience: mapping makes it possible to identifier the organization's key activities to definie a business continuity plan and is an essential tool for crisis management, whether digital or not.

Mercator

Composition of a map

1. Business

- The ecosystem view presents the different entities or systems with which the IS interacts to fulfill its function.
- The business view of the information system represents the IS through its main processes and information.

2. Application

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

3. Infrastructure

- The logical infrastructure view illustrates the logical partitioning of networks, including the definition of IP address ranges, VLANs, and filtering and routing functions ;
- The physical infrastructure view describes the physical equipment that are used by the information system.

Mercator

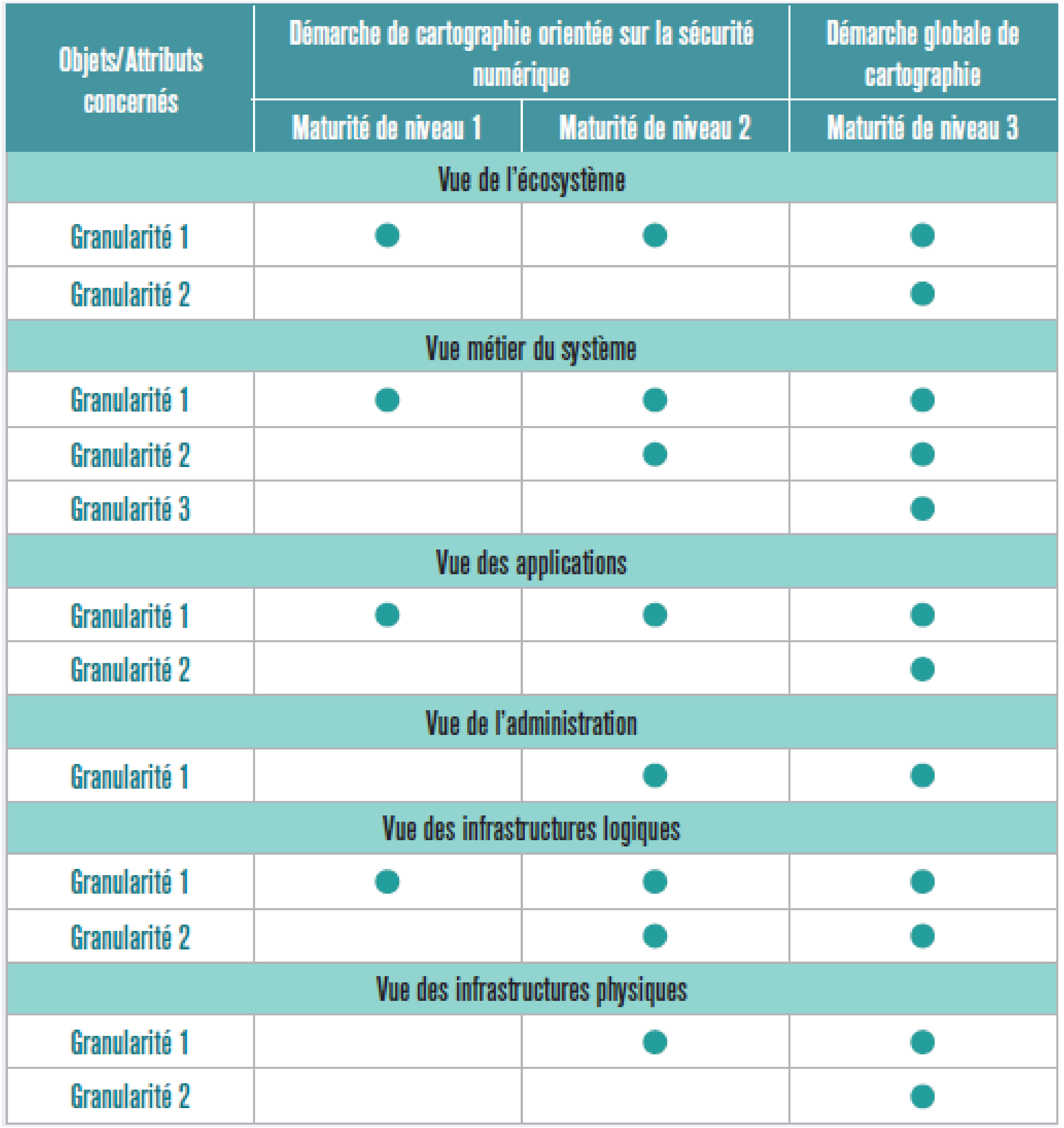
Levels of granularity

Each step has its own level of granularity.

Minimum granularity level 1:
Initial elements essential to digital security operations

Intermediate level 2 granularity:
Digital security oriented mapping. Vital information systems must have a mapping with this minimum level of maturity.

Level 3 fine granularity:
Comprehensive and detailed mapping that incorporates digital security requirements.



Objets/Attributs concernés	Démarche de cartographie orientée sur la sécurité numérique		Démarche globale de cartographie
	Maturité de niveau 1	Maturité de niveau 2	Maturité de niveau 3
Vue de l'écosystème			
Granularité 1	●	●	●
Granularité 2			●
Vue métier du système			
Granularité 1	●	●	●
Granularité 2		●	●
Granularité 3			●
Vue des applications			
Granularité 1	●	●	●
Granularité 2			●
Vue de l'administration			
Granularité 1		●	●
Vue des infrastructures logiques			
Granularité 1	●	●	●
Granularité 2		●	●
Vue des infrastructures physiques			
Granularité 1		●	●
Granularité 2			●

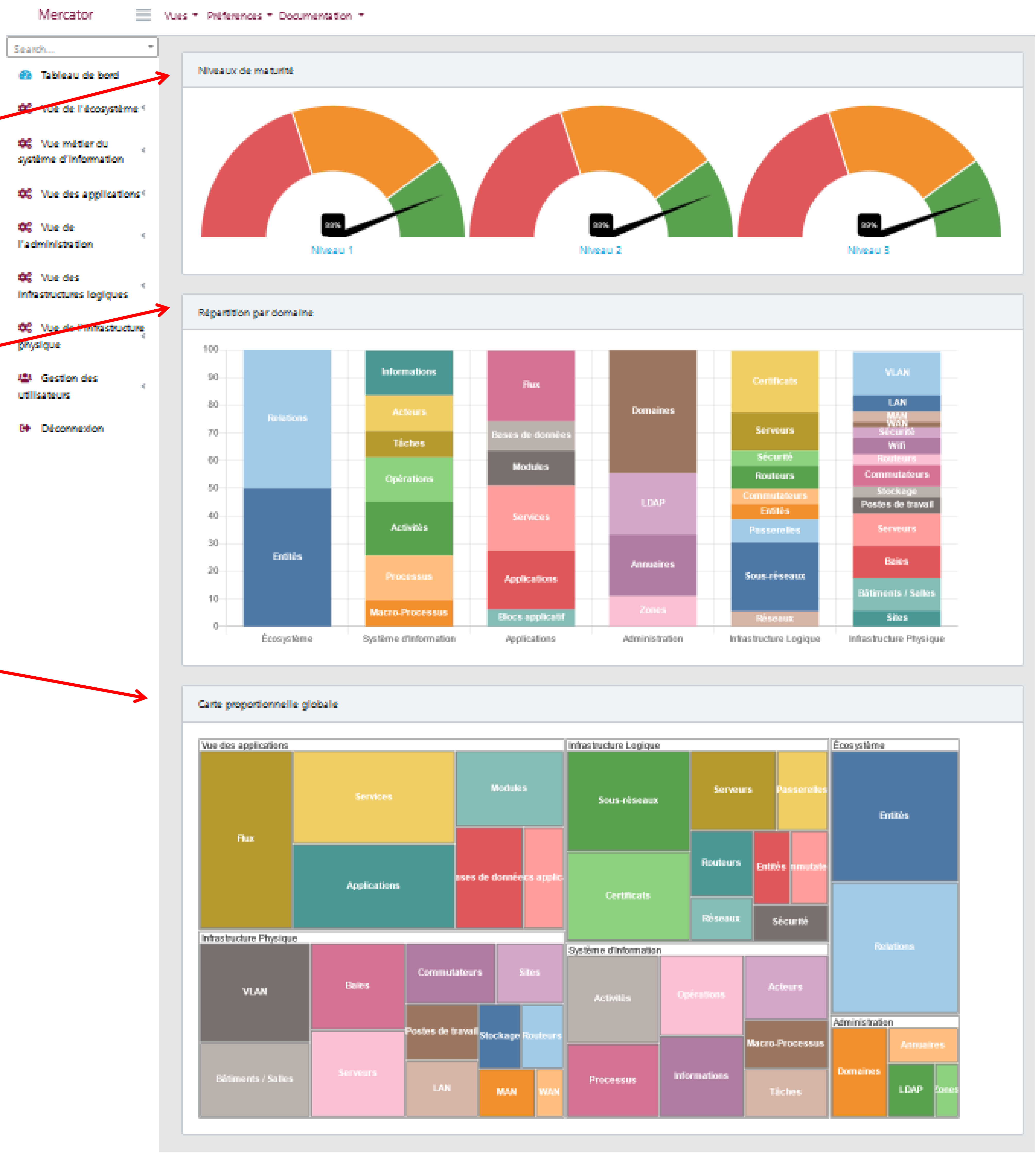
Mercator

Main screen

- Maturity level

- Breakdown by domain

- Global proportional map



Mercator

Top panel

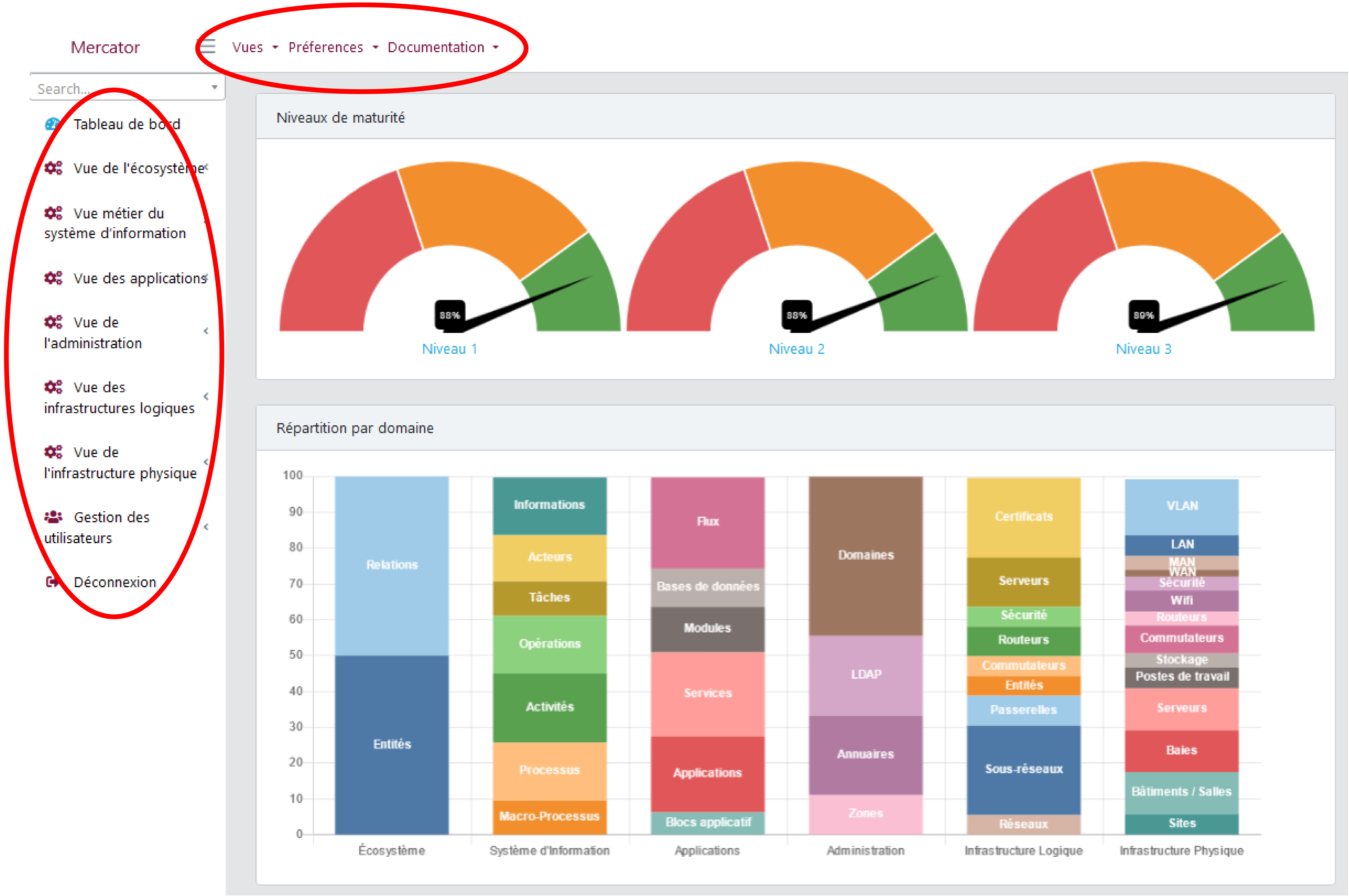
- Views

- Preferences

- Documentation

Left panel

- Data entry



Mercator

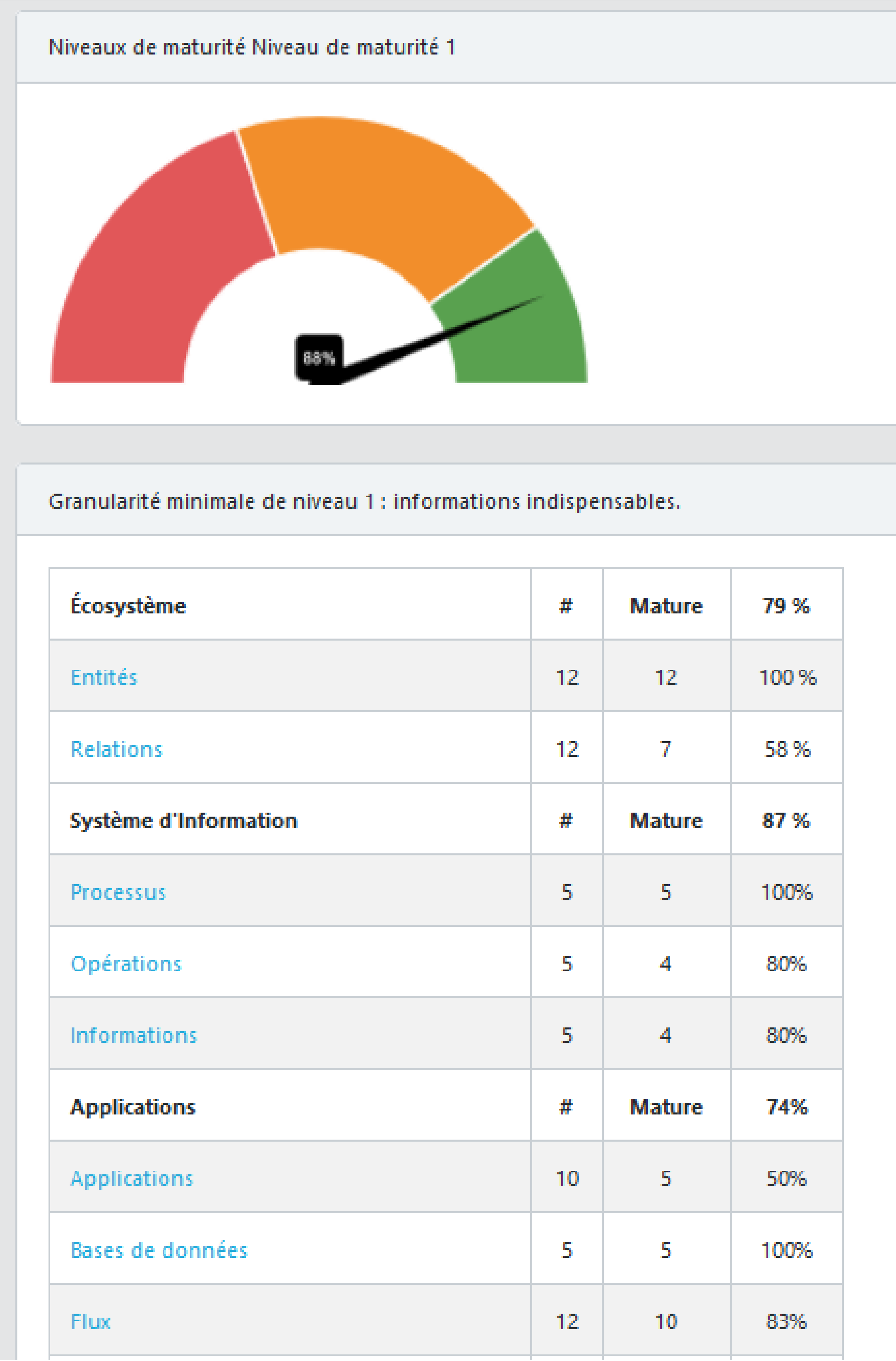
Computing the maturity level

Presence of information :
- no description
- no responsible
- no type ...

Links between assets :
- entity without relations
- process without operations
- application that does not support any process
- server without applications

Computation :
conforming assets / total number of assets

% represents the effort to be compliant



Niveaux de maturité Niveau de maturité 1

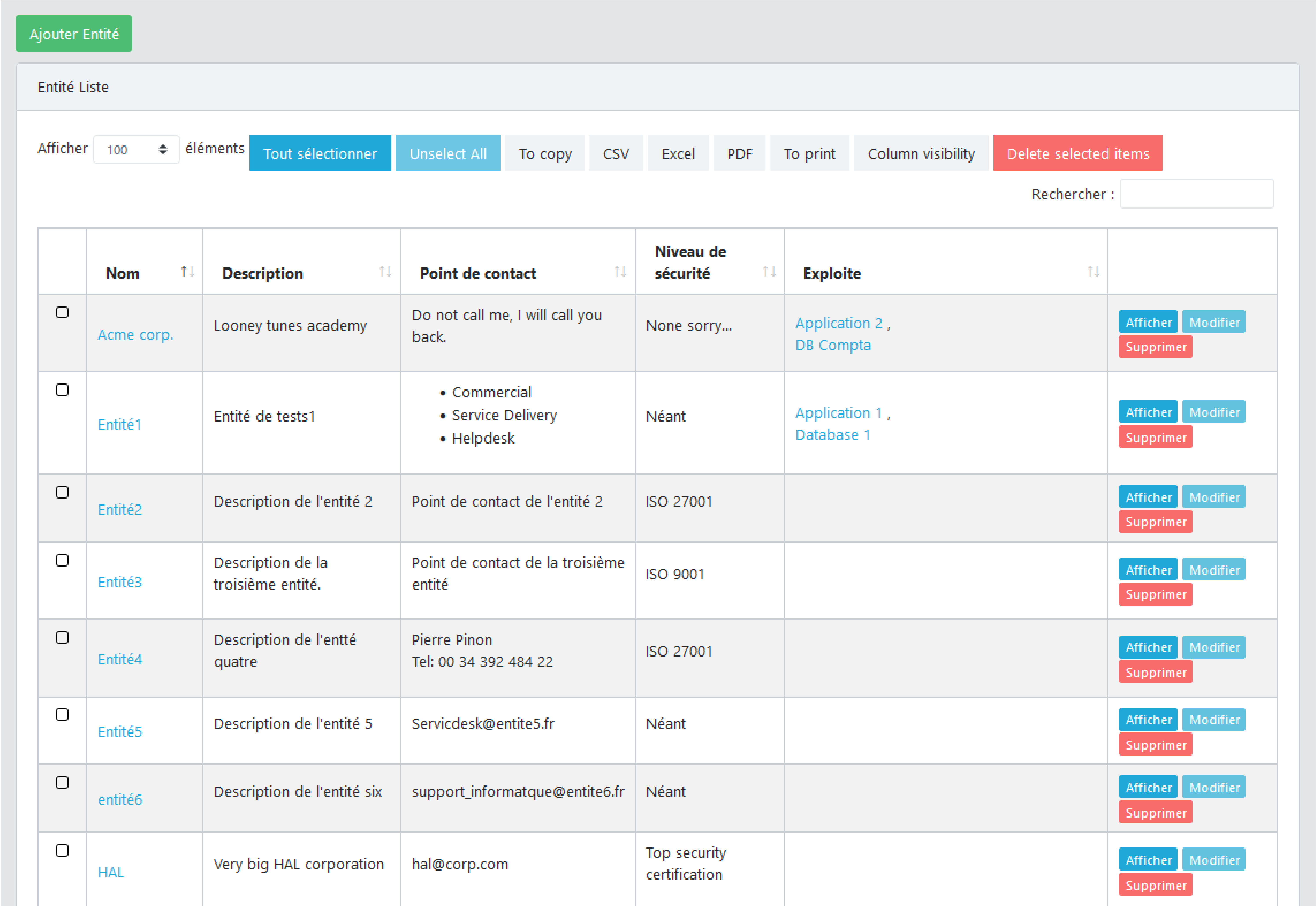
Granularité minimale de niveau 1 : informations indispensables.

Écosystème	#	Mature	79 %
Entités	12	12	100 %
Relations	12	7	58 %
Système d'Information	**#**	**Mature**	**87 %**
Processus	5	5	100%
Opérations	5	4	80%
Informations	5	4	80%
Applications	**#**	**Mature**	**74%**
Applications	10	5	50%
Bases de données	5	5	100%
Flux	12	10	83%

Mercator

Lists

- Sort on each column
- Search for
- Hide a column
- Show / Modify / Delete
- Copy
- Print
- Export : Excel, PDF, CSV, ...

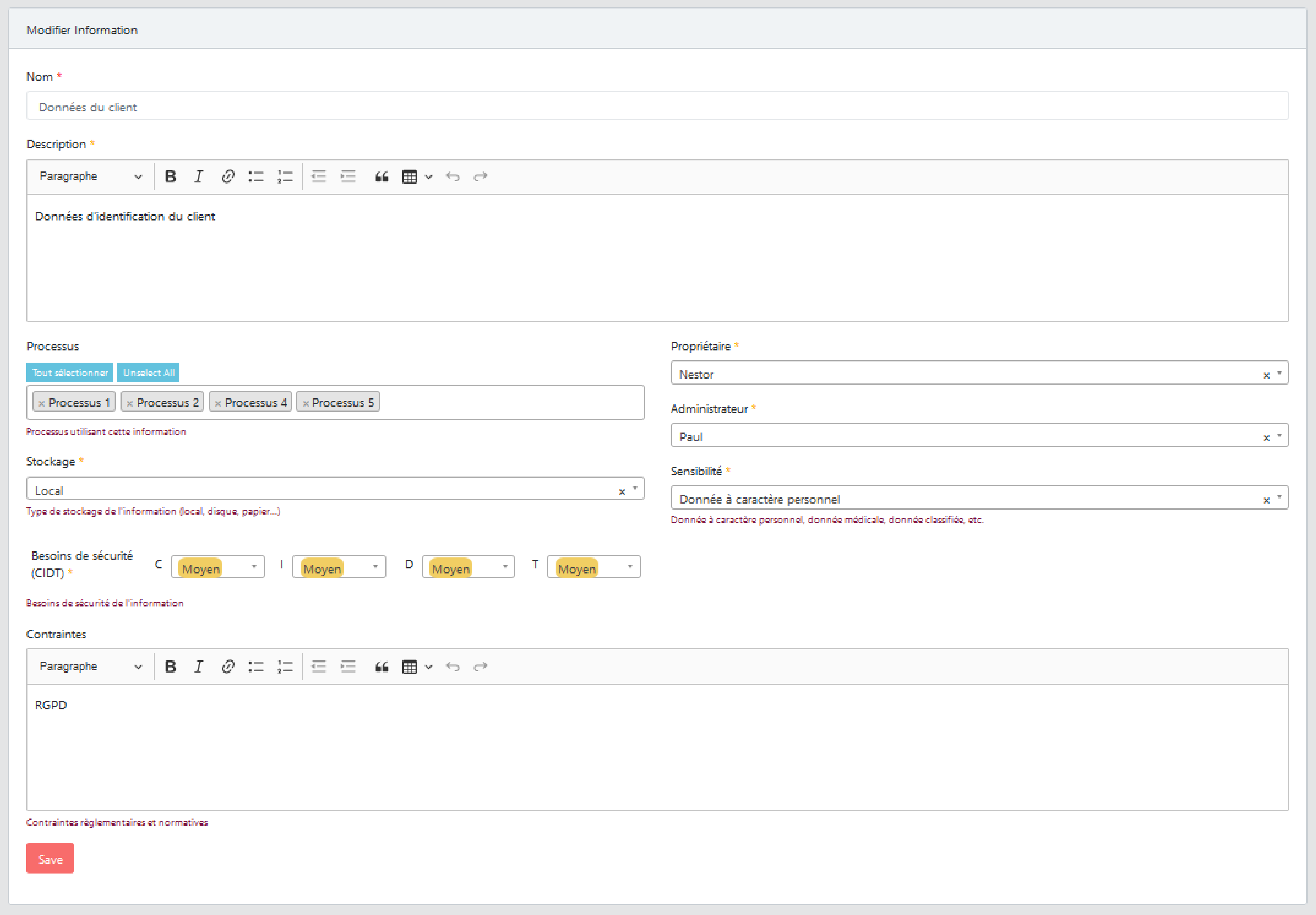


	Nom	Description	Point de contact	Niveau de sécurité	Exploite	
□	Acme corp.	Looney tunes academy	Do not call me, I will call you back.	None sorry...	Application 2 , DB Compta	Afficher Modifier Supprimer
□	Entité1	Entité de tests1	• Commercial • Service Delivery • Helpdesk	Néant	Application 1 , Database 1	Afficher Modifier Supprimer
□	Entité2	Description de l'entité 2	Point de contact de l'entité 2	ISO 27001		Afficher Modifier Supprimer
□	Entité3	Description de la troisième entité.	Point de contact de la troisième entité	ISO 9001		Afficher Modifier Supprimer
□	Entité4	Description de l'entté quatre	Pierre Pinon Tel: 00 34 392 484 22	ISO 27001		Afficher Modifier Supprimer
□	Entité5	Description de l'entité 5	Servicdesk@entite5.fr	Néant		Afficher Modifier Supprimer
□	entité6	Description de l'entité six	support_informatque@entite6.fr	Néant		Afficher Modifier Supprimer
□	HAL	Very big HAL corporation	hal@corp.com	Top security certification		Afficher Modifier Supprimer

Mercator

Forms

- RFT Editor
- Drop-down list
- Links between objects
- Security requirements
- Roles management
- History of changes



Modifier Information

Nom *

Données du client

Description *

Données d'identification du client

Processus

× Processus 1 × Processus 2 × Processus 4 × Processus 5

Processus utilisant cette information

Stockage *

Local

Type de stockage de l'information (local, disque, papier…)

Propriétaire *

Nestor

Administrateur *

Paul

Sensibilité *

Donnée à caractère personnel

Donnée à caractère personnel, donnée médicale, donnée classifiée, etc.

Besoins de sécurité (CIDT) *

C	Moyen	I	Moyen	D	Moyen	T	Moyen

Besoins de sécurité de l'information

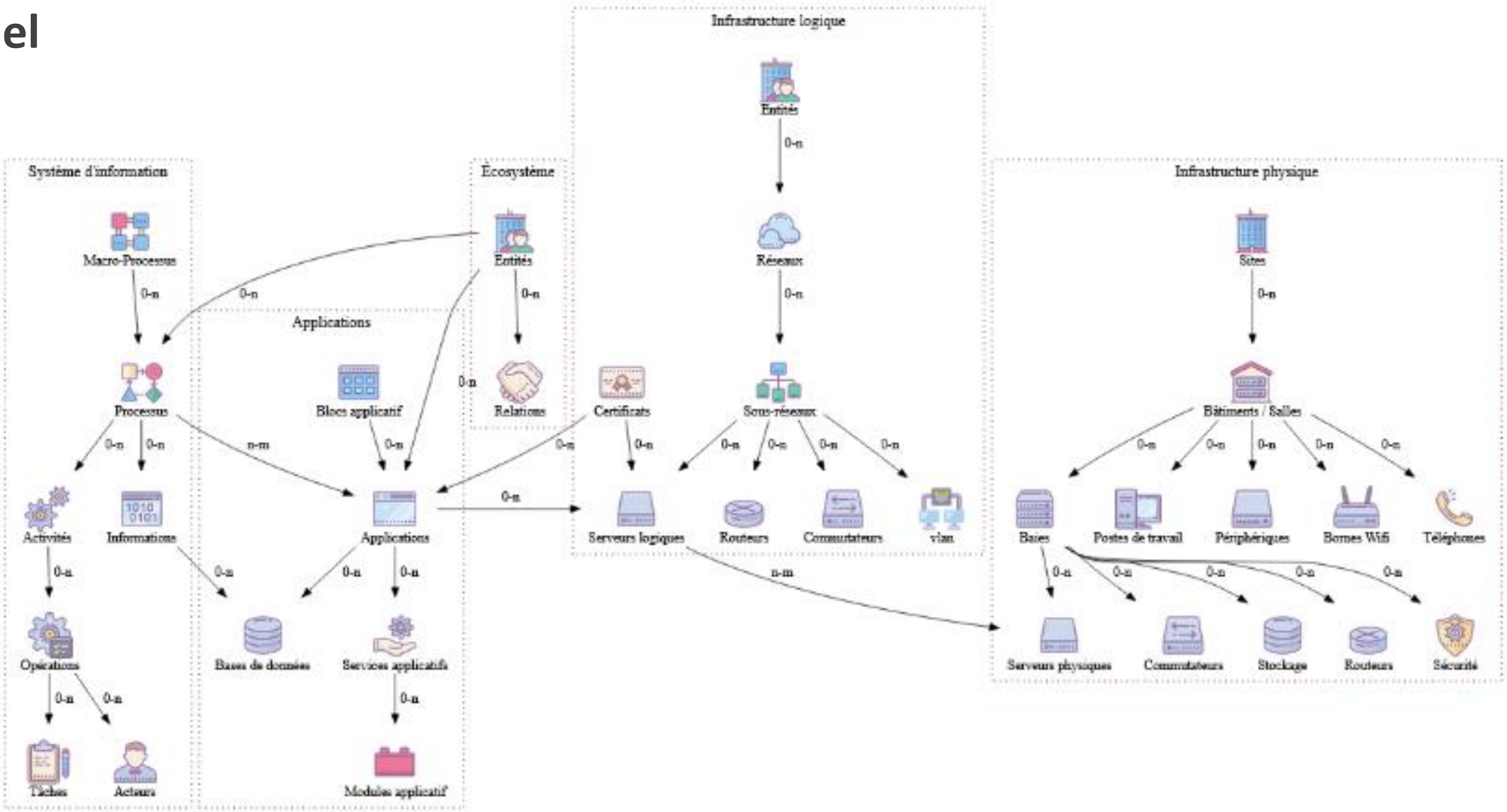
Contraintes

RGPD

Contraintes réglementaires et normatives

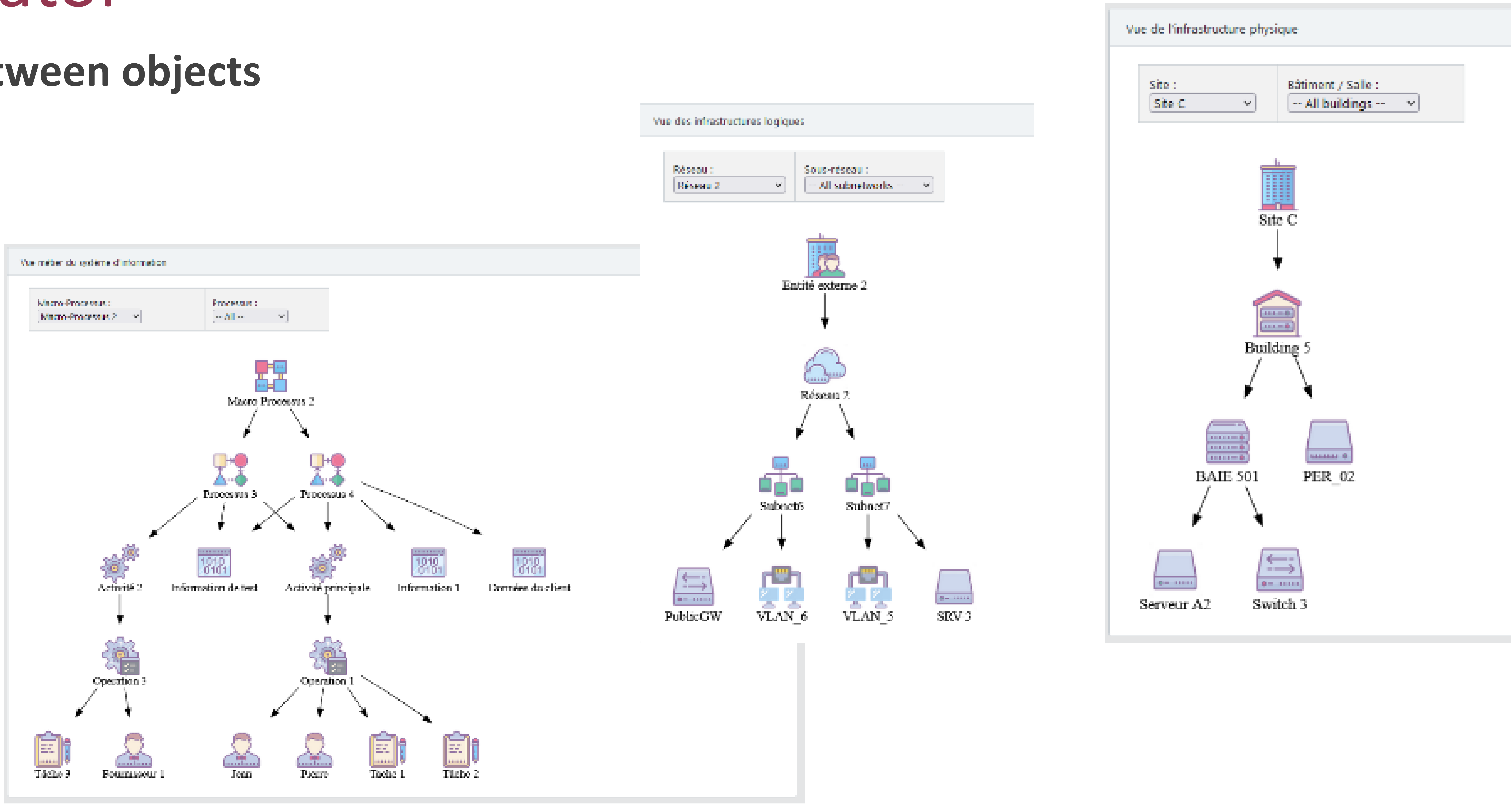
Mercator

Data Model



Mercator

Links between objects



Vue métier du système d'information

Macro-Processus : Macro-Processus 2

Processus : -- All --

Vue des infrastructures logiques

Réseau : Réseau 2

Sous-réseau : -- All subnetworks --

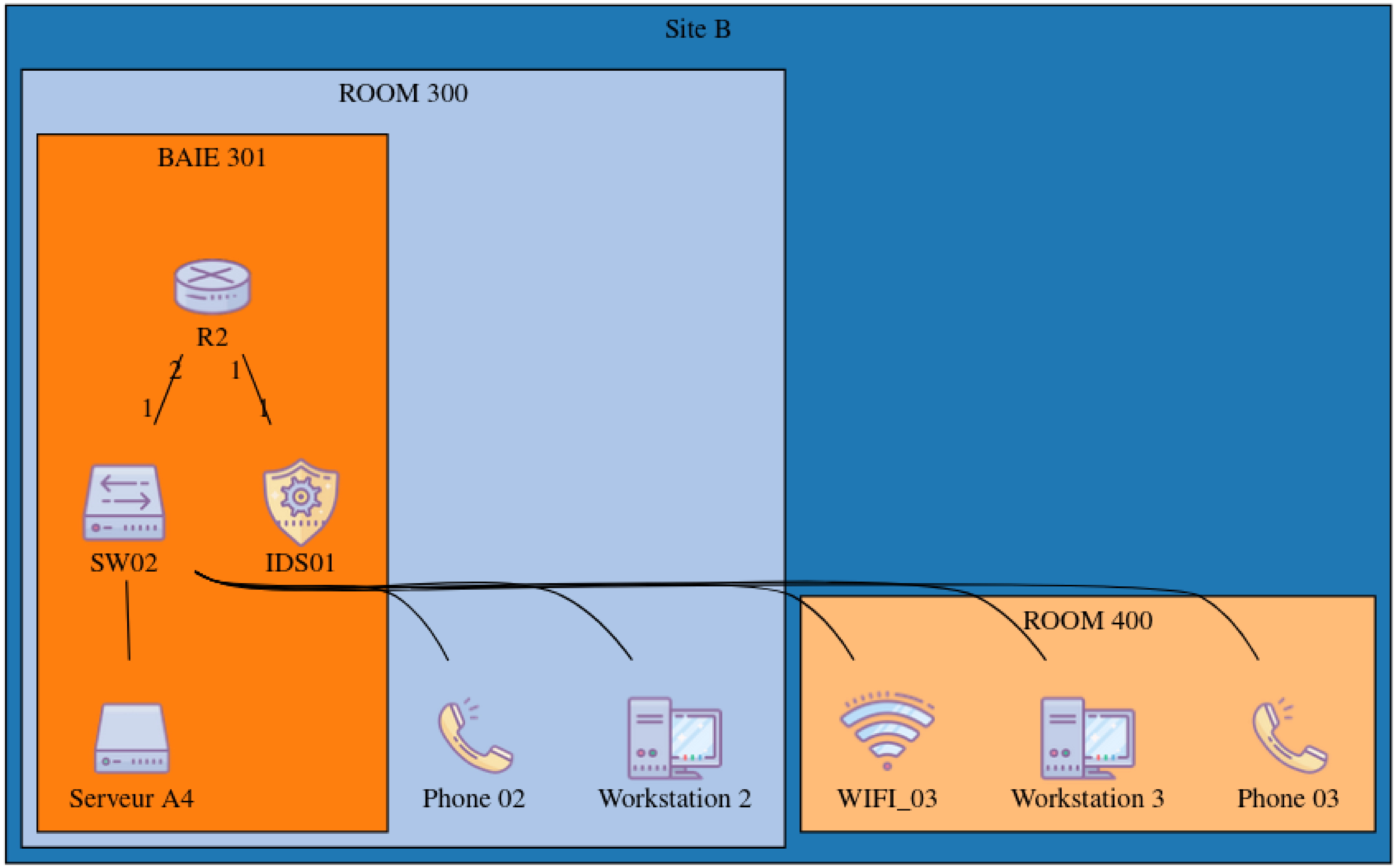
Vue de l'infrastructure physique

Site : Site C

Bâtiment / Salle : -- All buildings --

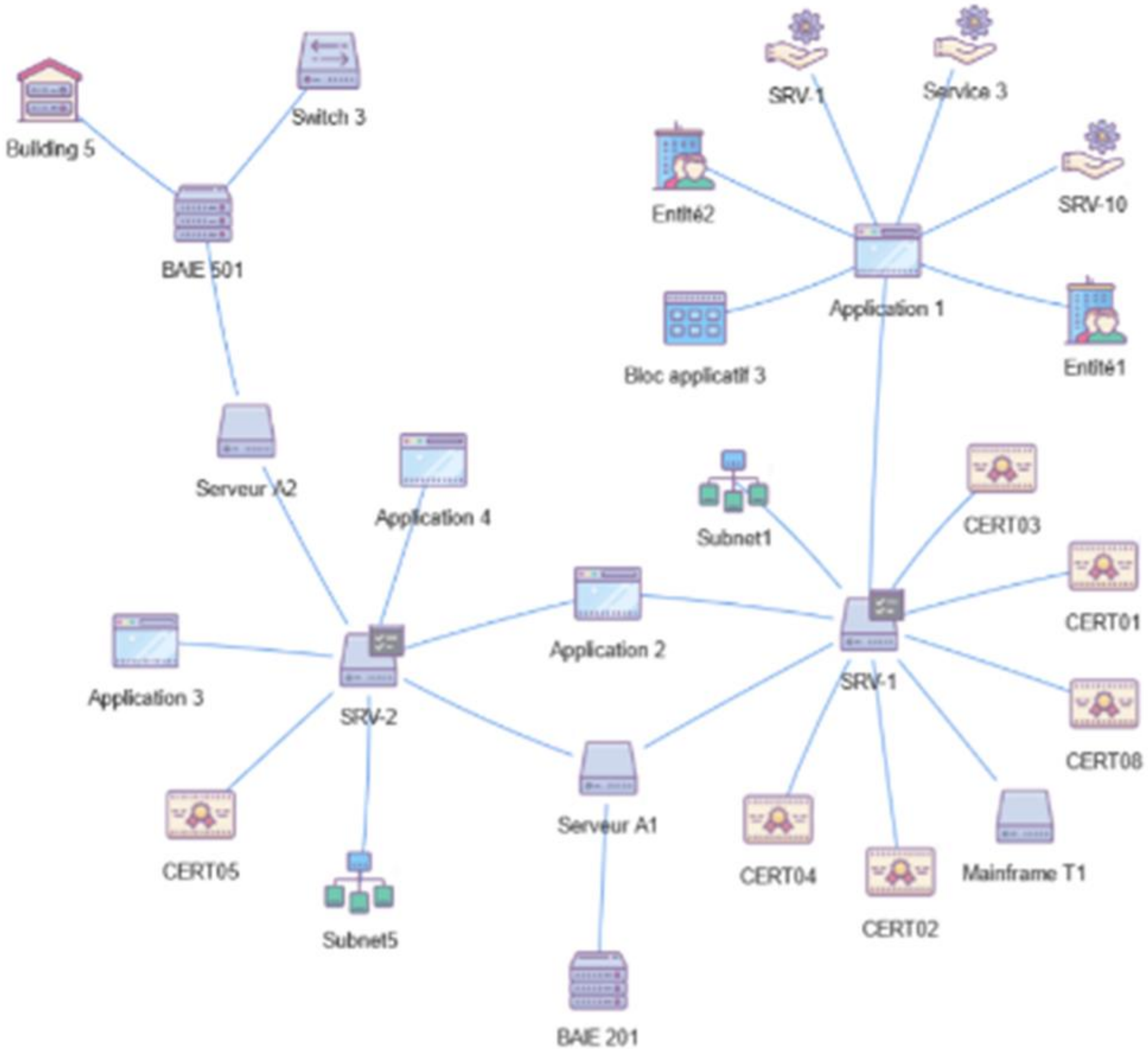
Mercator

Physical network schema



Mercator

Explore cartography



Mercator

Reports

Information System Mapping Report

Lists

Supported entities and applications
List of information system entities and their supported applications

Applications by application group
List of applications by application group

Logical servers
List of logical servers by applications and managers

Analysis of security needs
List of security needs between macro-processes, processes, applications, database and information.

Logical servers configuration
List of logical servers configuration

Inventory of the physical infrastructure
List of equipment by site/location

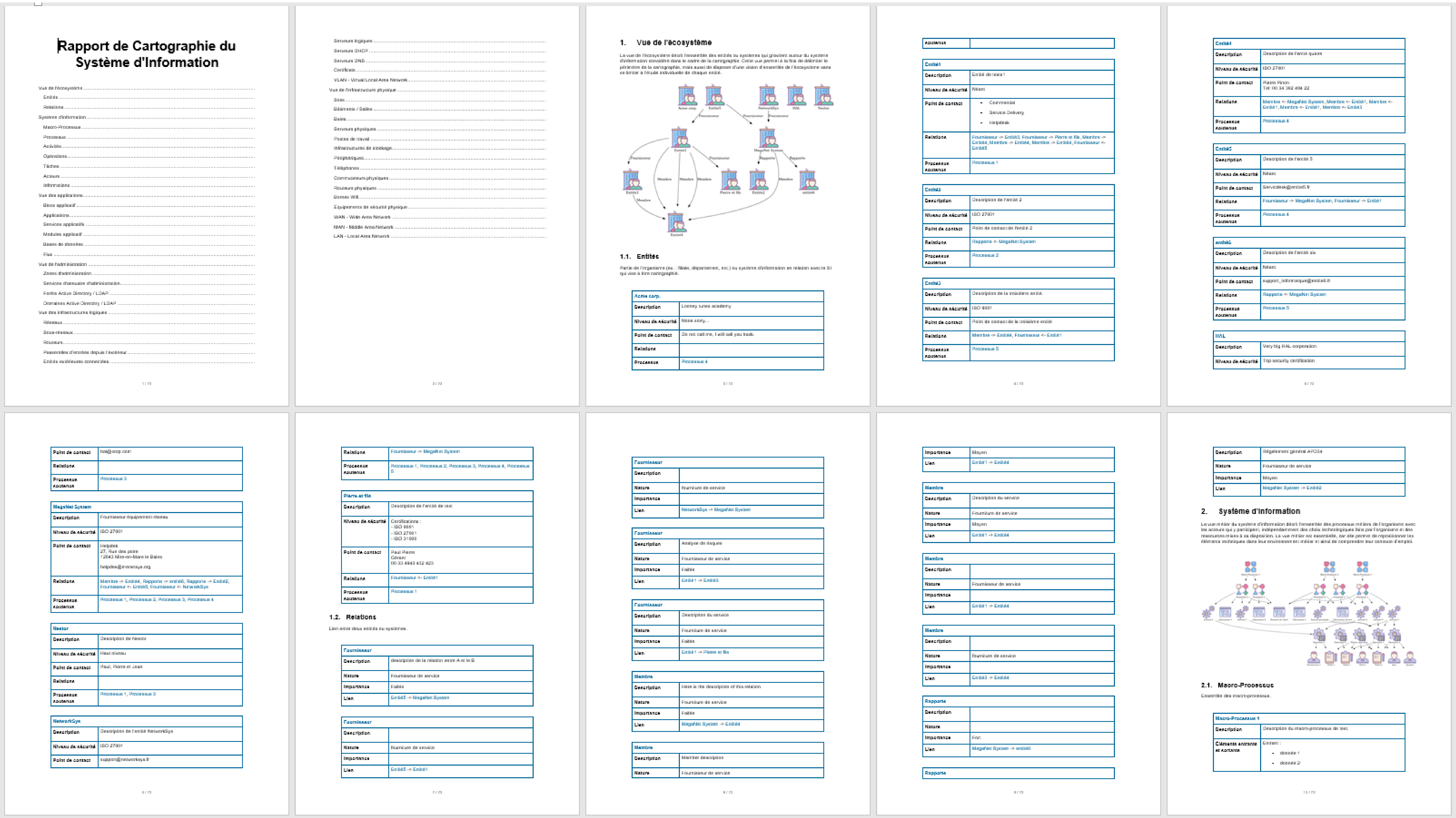
Audit

Maturity levels
Lists the maturity levels reached by the different objects of the mapping

Update / changes
Traces the changes made to the map in the last 12 months

Mercator

Information System Mapping Report



Rapport de Cartographie du Système d'Information

1. Vue de l'écosystème

La vue de l'écosystème décrit l'ensemble des entités ou systèmes qui gravitent autour du système d'information considéré dans le cadre de la cartographie. Cette vue permet à la fois de délimiter le périmètre de la cartographie, mais aussi de disposer d'une vision d'ensemble de l'écosystème sans se limiter à l'étude individuelle de chaque entité.

1.1. Entités

Partie de l'organisme (ex. : filiale, département, etc.) ou système d'information en relation avec le SI qui vise à être cartographié.

Acme corp.	
Description	Looney tunes academy
Niveau de sécurité	None sorry...
Point de contact	Do not call me, I will call you back.
Relations	
Processus	Processus 4

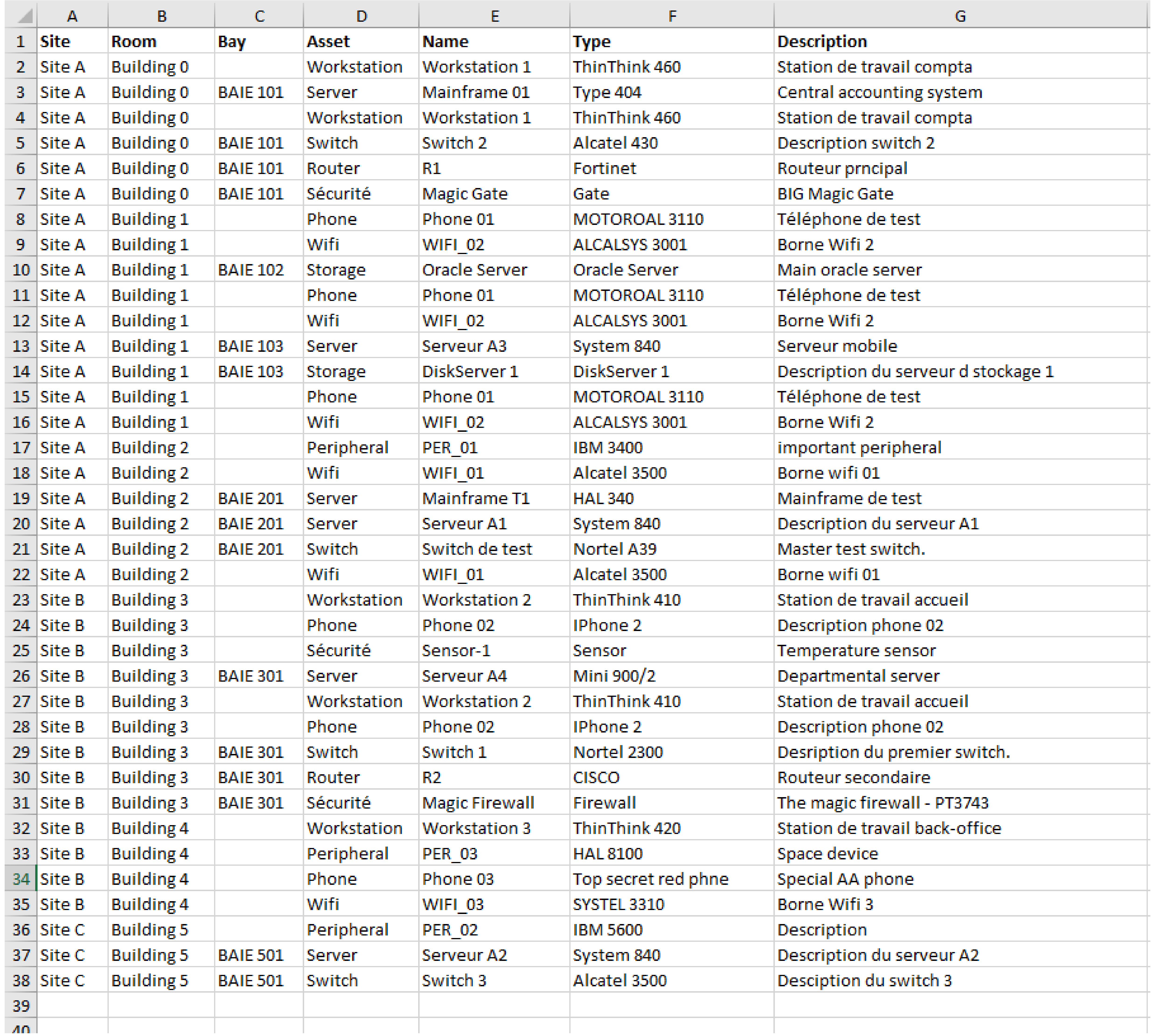
1.2. Relations

2. Système d'information

2.1. Macro-Processus

Mercator

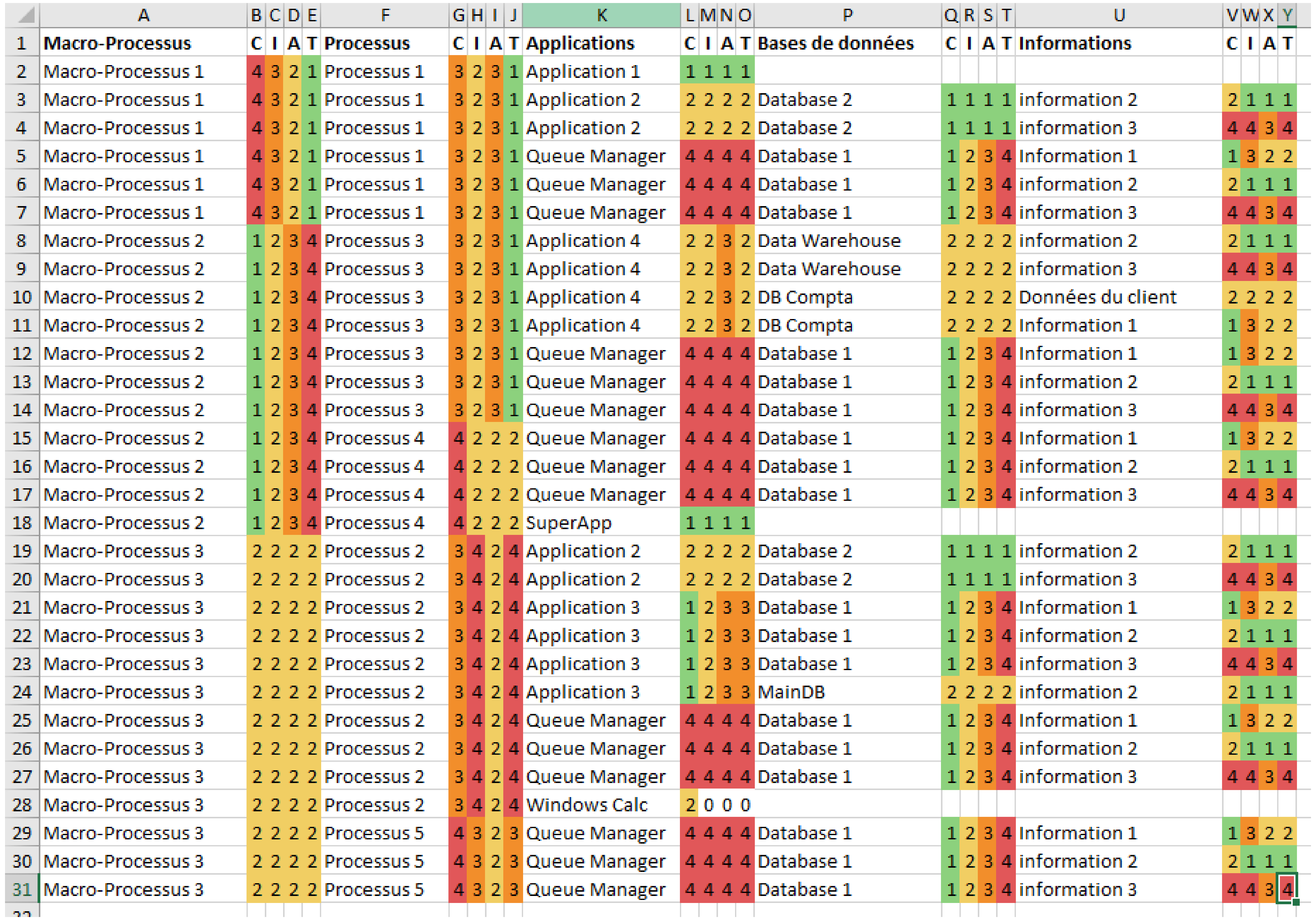
Physical inventory



	A	B	C	D	E	F	G
1	**Site**	**Room**	**Bay**	**Asset**	**Name**	**Type**	**Description**
2	Site A	Building 0		Workstation	Workstation 1	ThinThink 460	Station de travail compta
3	Site A	Building 0	BAIE 101	Server	Mainframe 01	Type 404	Central accounting system
4	Site A	Building 0		Workstation	Workstation 1	ThinThink 460	Station de travail compta
5	Site A	Building 0	BAIE 101	Switch	Switch 2	Alcatel 430	Description switch 2
6	Site A	Building 0	BAIE 101	Router	R1	Fortinet	Routeur prncipal
7	Site A	Building 0	BAIE 101	Sécurité	Magic Gate	Gate	BIG Magic Gate
8	Site A	Building 1		Phone	Phone 01	MOTOROAL 3110	Téléphone de test
9	Site A	Building 1		Wifi	WIFI_02	ALCALSYS 3001	Borne Wifi 2
10	Site A	Building 1	BAIE 102	Storage	Oracle Server	Oracle Server	Main oracle server
11	Site A	Building 1		Phone	Phone 01	MOTOROAL 3110	Téléphone de test
12	Site A	Building 1		Wifi	WIFI_02	ALCALSYS 3001	Borne Wifi 2
13	Site A	Building 1	BAIE 103	Server	Serveur A3	System 840	Serveur mobile
14	Site A	Building 1	BAIE 103	Storage	DiskServer 1	DiskServer 1	Description du serveur d stockage 1
15	Site A	Building 1		Phone	Phone 01	MOTOROAL 3110	Téléphone de test
16	Site A	Building 1		Wifi	WIFI_02	ALCALSYS 3001	Borne Wifi 2
17	Site A	Building 2		Peripheral	PER_01	IBM 3400	important peripheral
18	Site A	Building 2		Wifi	WIFI_01	Alcatel 3500	Borne wifi 01
19	Site A	Building 2	BAIE 201	Server	Mainframe T1	HAL 340	Mainframe de test
20	Site A	Building 2	BAIE 201	Server	Serveur A1	System 840	Description du serveur A1
21	Site A	Building 2	BAIE 201	Switch	Switch de test	Nortel A39	Master test switch.
22	Site A	Building 2		Wifi	WIFI_01	Alcatel 3500	Borne wifi 01
23	Site B	Building 3		Workstation	Workstation 2	ThinThink 410	Station de travail accueil
24	Site B	Building 3		Phone	Phone 02	IPhone 2	Description phone 02
25	Site B	Building 3		Sécurité	Sensor-1	Sensor	Temperature sensor
26	Site B	Building 3	BAIE 301	Server	Serveur A4	Mini 900/2	Departmental server
27	Site B	Building 3		Workstation	Workstation 2	ThinThink 410	Station de travail accueil
28	Site B	Building 3		Phone	Phone 02	IPhone 2	Description phone 02
29	Site B	Building 3	BAIE 301	Switch	Switch 1	Nortel 2300	Desription du premier switch.
30	Site B	Building 3	BAIE 301	Router	R2	CISCO	Routeur secondaire
31	Site B	Building 3	BAIE 301	Sécurité	Magic Firewall	Firewall	The magic firewall - PT3743
32	Site B	Building 4		Workstation	Workstation 3	ThinThink 420	Station de travail back-office
33	Site B	Building 4		Peripheral	PER_03	HAL 8100	Space device
34	Site B	Building 4		Phone	Phone 03	Top secret red phne	Special AA phone
35	Site B	Building 4		Wifi	WIFI_03	SYSTEL 3310	Borne Wifi 3
36	Site C	Building 5		Peripheral	PER_02	IBM 5600	Description
37	Site C	Building 5	BAIE 501	Server	Serveur A2	System 840	Description du serveur A2
38	Site C	Building 5	BAIE 501	Switch	Switch 3	Alcatel 3500	Desciption du switch 3
39							
40							

Mercator

Analysis of the security needs



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1	**Macro-Processus**	**C**	**I**	**A**	**T**	**Processus**	**C**	**I**	**A**	**T**	**Applications**	**C**	**I**	**A**	**T**	**Bases de données**	**C**	**I**	**A**	**T**	**Informations**	**C**	**I**	**A**	**T**
2	Macro-Processus 1	4	3	2	1	Processus 1	3	2	3	1	Application 1	1	1	1	1										
3	Macro-Processus 1	4	3	2	1	Processus 1	3	2	3	1	Application 2	2	2	2	2	Database 2	1	1	1	1	information 2	2	1	1	1
4	Macro-Processus 1	4	3	2	1	Processus 1	3	2	3	1	Application 2	2	2	2	2	Database 2	1	1	1	1	information 3	4	4	3	4
5	Macro-Processus 1	4	3	2	1	Processus 1	3	2	3	1	Queue Manager	4	4	4	4	Database 1	1	2	3	4	Information 1	1	3	2	2
6	Macro-Processus 1	4	3	2	1	Processus 1	3	2	3	1	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 2	2	1	1	1
7	Macro-Processus 1	4	3	2	1	Processus 1	3	2	3	1	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 3	4	4	3	4
8	Macro-Processus 2	1	2	3	4	Processus 3	3	2	3	1	Application 4	2	2	3	2	Data Warehouse	2	2	2	2	information 2	2	1	1	1
9	Macro-Processus 2	1	2	3	4	Processus 3	3	2	3	1	Application 4	2	2	3	2	Data Warehouse	2	2	2	2	information 3	4	4	3	4
10	Macro-Processus 2	1	2	3	4	Processus 3	3	2	3	1	Application 4	2	2	3	2	DB Compta	2	2	2	2	Données du client	2	2	2	2
11	Macro-Processus 2	1	2	3	4	Processus 3	3	2	3	1	Application 4	2	2	3	2	DB Compta	2	2	2	2	Information 1	1	3	2	2
12	Macro-Processus 2	1	2	3	4	Processus 3	3	2	3	1	Queue Manager	4	4	4	4	Database 1	1	2	3	4	Information 1	1	3	2	2
13	Macro-Processus 2	1	2	3	4	Processus 3	3	2	3	1	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 2	2	1	1	1
14	Macro-Processus 2	1	2	3	4	Processus 3	3	2	3	1	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 3	4	4	3	4
15	Macro-Processus 2	1	2	3	4	Processus 4	4	2	2	2	Queue Manager	4	4	4	4	Database 1	1	2	3	4	Information 1	1	3	2	2
16	Macro-Processus 2	1	2	3	4	Processus 4	4	2	2	2	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 2	2	1	1	1
17	Macro-Processus 2	1	2	3	4	Processus 4	4	2	2	2	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 3	4	4	3	4
18	Macro-Processus 2	1	2	3	4	Processus 4	4	2	2	2	SuperApp	1	1	1	1										
19	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Application 2	2	2	2	2	Database 2	1	1	1	1	information 2	2	1	1	1
20	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Application 2	2	2	2	2	Database 2	1	1	1	1	information 3	4	4	3	4
21	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Application 3	1	2	3	3	Database 1	1	2	3	4	Information 1	1	3	2	2
22	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Application 3	1	2	3	3	Database 1	1	2	3	4	information 2	2	1	1	1
23	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Application 3	1	2	3	3	Database 1	1	2	3	4	information 3	4	4	3	4
24	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Application 3	1	2	3	3	MainDB	2	2	2	2	information 2	2	1	1	1
25	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Queue Manager	4	4	4	4	Database 1	1	2	3	4	Information 1	1	3	2	2
26	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 2	2	1	1	1
27	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 3	4	4	3	4
28	Macro-Processus 3	2	2	2	2	Processus 2	3	4	2	4	Windows Calc	2	0	0	0										
29	Macro-Processus 3	2	2	2	2	Processus 5	4	3	2	3	Queue Manager	4	4	4	4	Database 1	1	2	3	4	Information 1	1	3	2	2
30	Macro-Processus 3	2	2	2	2	Processus 5	4	3	2	3	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 2	2	1	1	1
31	Macro-Processus 3	2	2	2	2	Processus 5	4	3	2	3	Queue Manager	4	4	4	4	Database 1	1	2	3	4	information 3	4	4	3	4

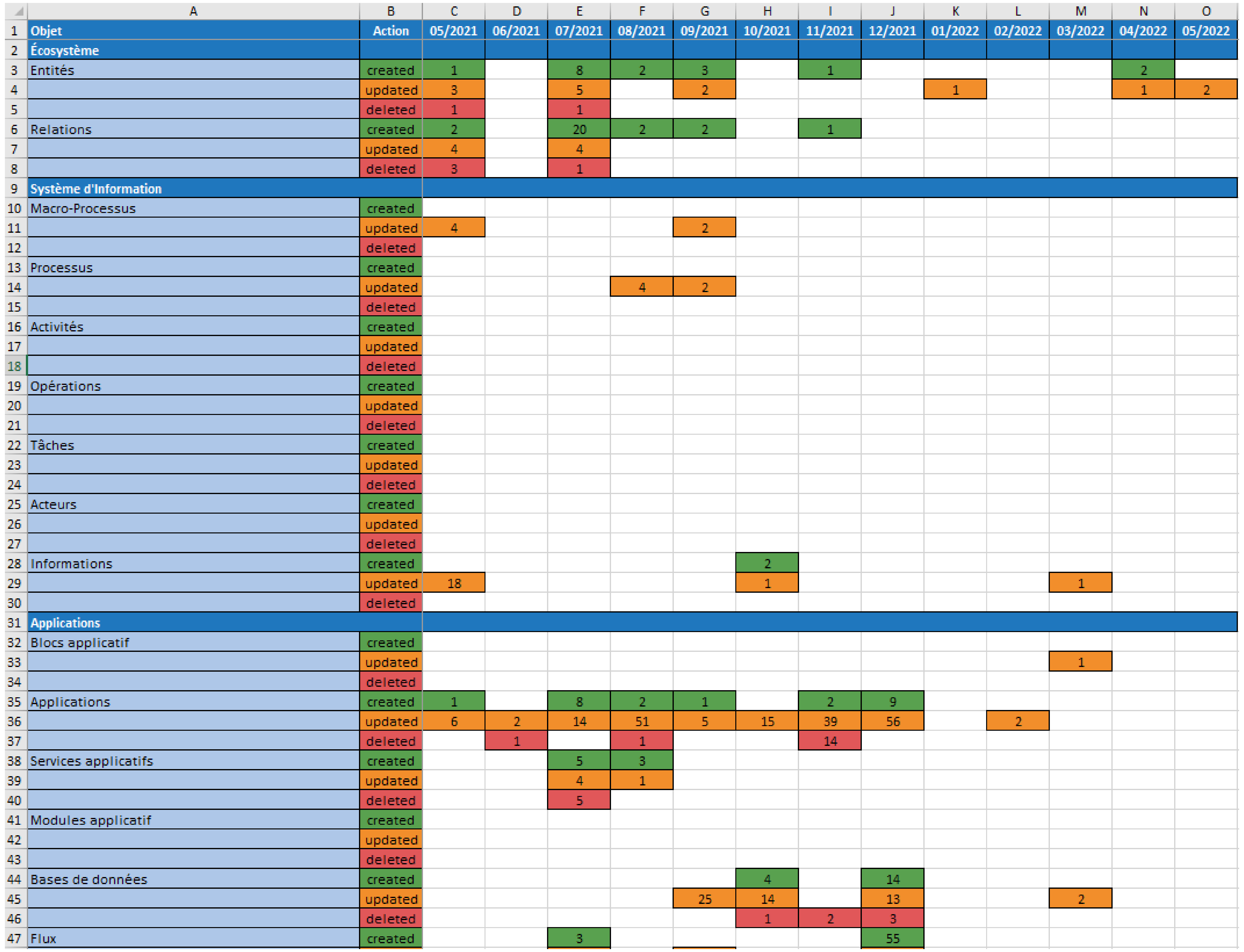
Analysis of the security needs

Denormalize the links between macro-processes, processes, applications, databases and information

Analyze the differences in requirements between each object.

Mercator

Cartography updates



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Objet	Action	05/2021	06/2021	07/2021	08/2021	09/2021	10/2021	11/2021	12/2021	01/2022	02/2022	03/2022	04/2022	05/2022
2	Écosystème														
3	Entités	created	1		8	2	3		1					2	
4		updated	3		5		2				1			1	2
5		deleted	1		1										
6	Relations	created	2		20	2	2		1						
7		updated	4		4										
8		deleted	3		1										
9	Système d'Information														
10	Macro-Processus	created													
11		updated	4				2								
12		deleted													
13	Processus	created													
14		updated				4	2								
15		deleted													
16	Activités	created													
17		updated													
18		deleted													
19	Opérations	created													
20		updated													
21		deleted													
22	Tâches	created													
23		updated													
24		deleted													
25	Acteurs	created													
26		updated													
27		deleted													
28	Informations	created						2							
29		updated	18					1					1		
30		deleted													
31	Applications														
32	Blocs applicatif	created													
33		updated											1		
34		deleted													
35	Applications	created	1		8	2	1		2	9					
36		updated	6	2	14	51	5	15	39	56		2			
37		deleted		1		1			14						
38	Services applicatifs	created			5	3									
39		updated			4	1									
40		deleted			5										
41	Modules applicatif	created													
42		updated													
43		deleted													
44	Bases de données	created						4		14					
45		updated					25	14		13			2		
46		deleted						1	2	3					
47	Flux	created			3					55					

Track the changes made to the mapping over the last 12 months

Track the updating of the map

Demonstrate that the mapping is updated regularly

Mercator

Links with ISO 27001:2013

Section	Titre
A8.1.1	Inventory of assets
A.8.1.2	Ownership of assets
A.8.2.1	Labelling of information
A.11.2.1	Location and protection of assets
A.12.1.2	Change management
A.12.1.3	Capacity management
A.12.6.1	Vulnerability management
A.13.1.3	Segregation of networks
A.15.1.2	Security in supplier agreements
A.16.1.4	Assessment of information security events
A.17.2.1	Availability of information processing resources

Mercator

Application available on GitHub https://github.com/dbarzin/mercator
under Open Source License

Usage
3 hospitals in Luxembourg
10 hospitals in France
3 administrations of French municipalities

Contributions
10 contributors

Roadmap
Treatment registry (GDPR), crisis directory, link with Monarc