Introduction to MONARC

Optimised Risk Analysis Method

Luxembourg House of Cybersecurity / NC3

National Cybersecurity Competence Centre of Luxembourg

May 31, 2023

- 2003: Cyberworld Awareness and Security Enhancement Services (**CASES**);
- 2007: Computer Incident Response Center Luxembourg (**CIRCL**);
- 2010: SECURITYMADEIN.LU is a *GIE* (Groupement d'Intérêt Économique). CIRCL and CASES are department of SECURITYMADEIN.LU;
- 2017: Cyber security Competence Center (**C3**), a new department of SECURITYMADEIN.LU;
- On 17th Oct. 2022: SECURITYMADEIN.LU transformed into the Luxembourg House of Cybersecurity (**LHC**)
  CASES and C3 are now the National Cybersecurity Competence Centre of Luxembourg (**NC3**)

CASES was an initiative of the Ministry of Economy after the worm *I love you* decimated more than 3 millions computers in less than a week.

Content at glance

1. What is MONARC?
2. The method
3. The tool

Summary

An open source software

MONARC is the tool you need for an optimised, precise and repeatable risk assessment.

- Web application (SaaS, self-hosted, virtual machine, etc.);
- source code[1]: `GNU Affero General Public License version 3`;
- data: `CC0 1.0 Universal - Public Domain Dedication`.

MONARC is easy to use.
Used and recognized by experts from different fields (not only information security).

For many users, it started with a spreadsheet!

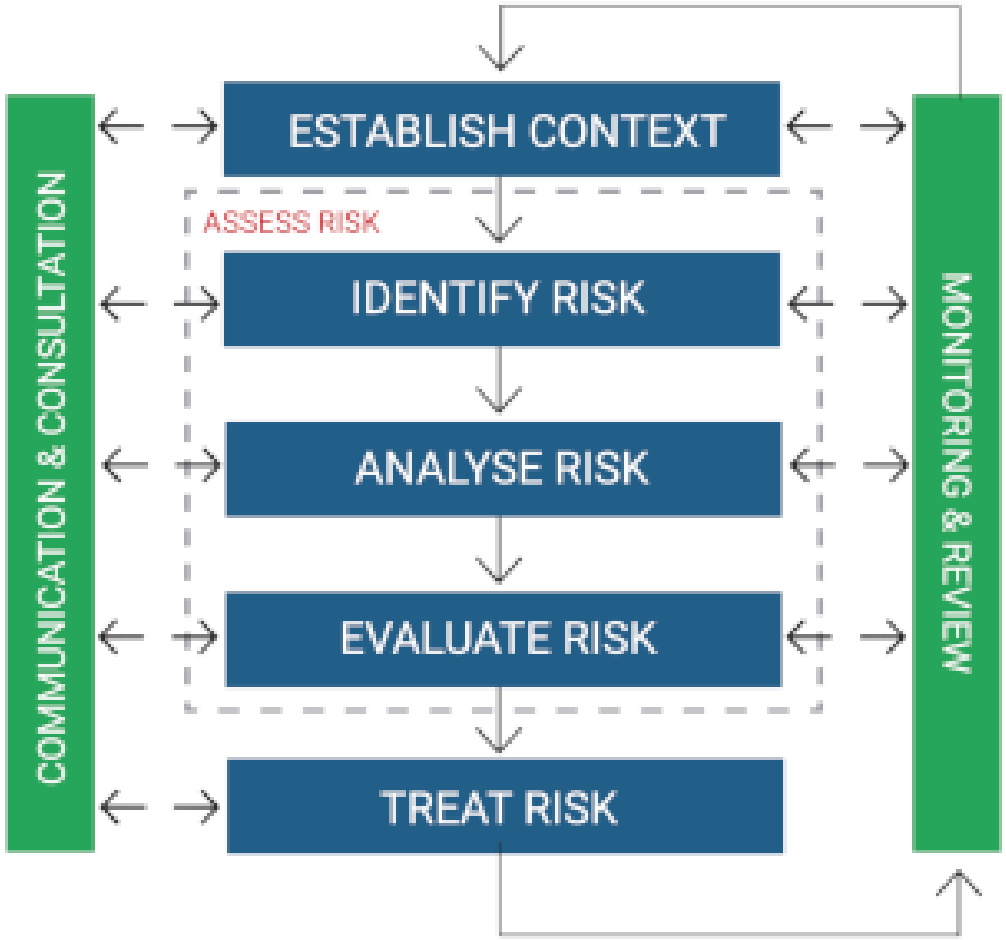
[1] `https://github.com/monarc-project`

A community

- more than 280 organizations:
  `https://my.monarc.lu`;
- 17 organizations sharing MONARC objects (threats, assets, recommendations, etc.):
  `https://objects.monarc.lu`;
- a global dashboard with trends about threats and vulnerabilitties:
  `https://dashboard.monarc.lu`;
- discussions on GitHub:
  `https://github.com/monarc-project/MonarcAppFO/discussions`.

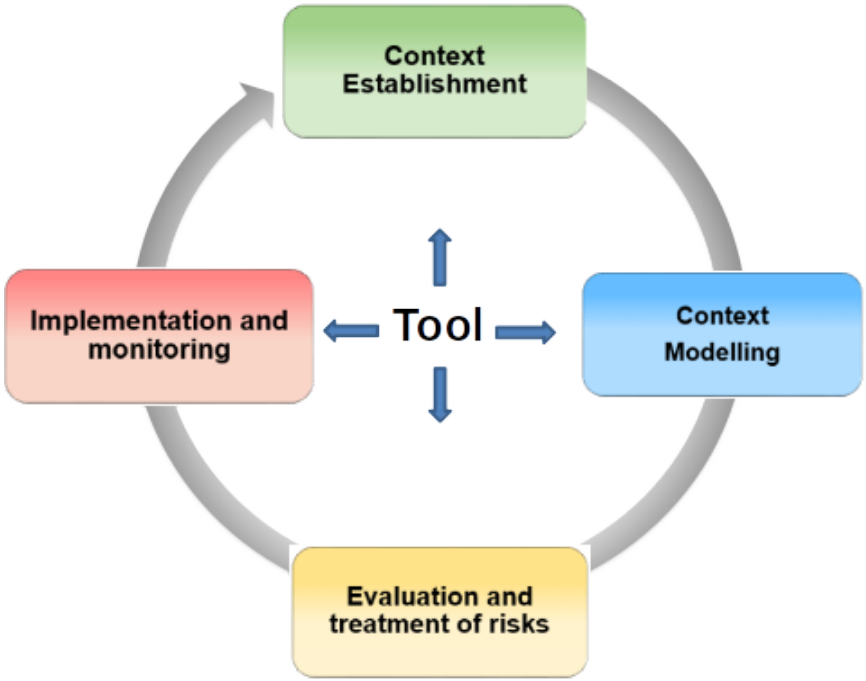
A method

Based on ISO/IEC 27005:2011, but optimized



Summary

A Structured, Iterative and Qualitative method

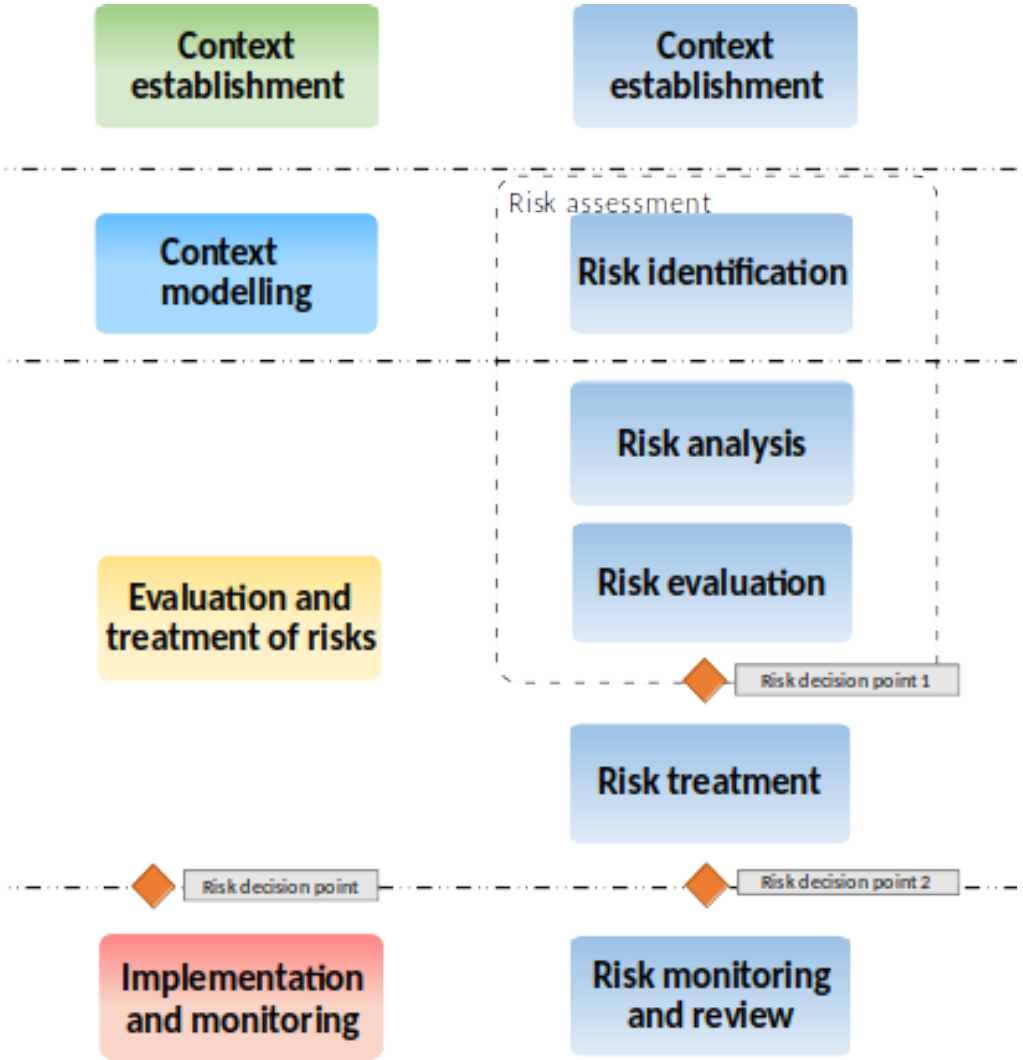


- Structured: 1, 2, ..., n.
- Iterative: **Plan**, **Do**, **Check**, **Act**
- Qualitative: **Values** / **Consequence**
  - Impact/Consequence, Threat, Vulnerability;
  - **r**eputation, image;
  - **o**peration;
  - **l**egal;
  - **f**inancial;
  - **p**erson (to the).

Possibility to define custom scales for operational risks.

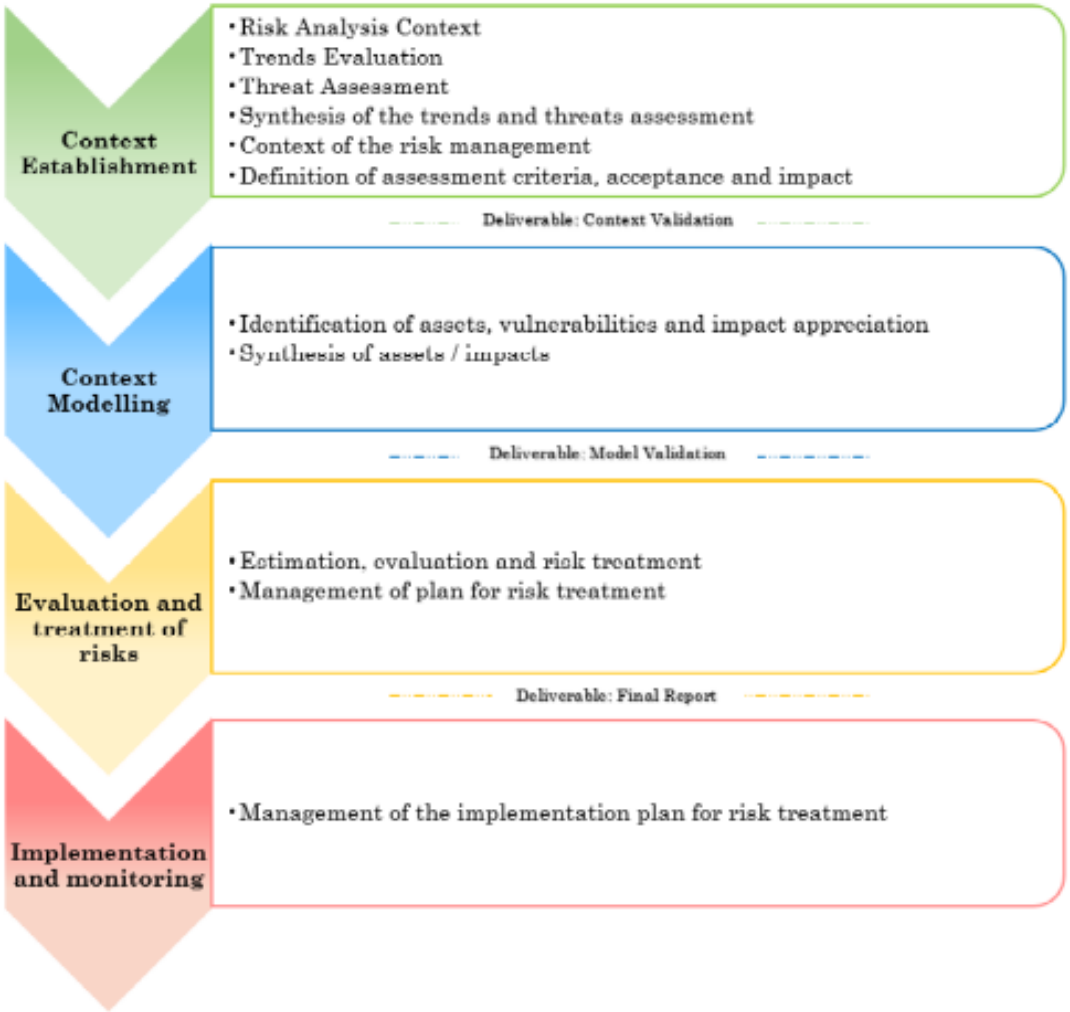
Automated and simplified management

Method based on ISO/IEC 27005



Automated and simplified management

Sub-stages provided by the method are also in line with ISO/IEC 27005



Information risks

$$R = \mathbf{I}mpact \times \mathbf{T}hreat \times \mathbf{V}ulnerability$$

- impact on **C**onfidentiality **I**ntegrity **A**vailability;
- on secondary assets.

Operational risks

$$R = \mathbf{I}mpact \times \mathbf{P}robability$$

- impact by default on ROLFP (possibility to define custom scales);
- on primary assets.

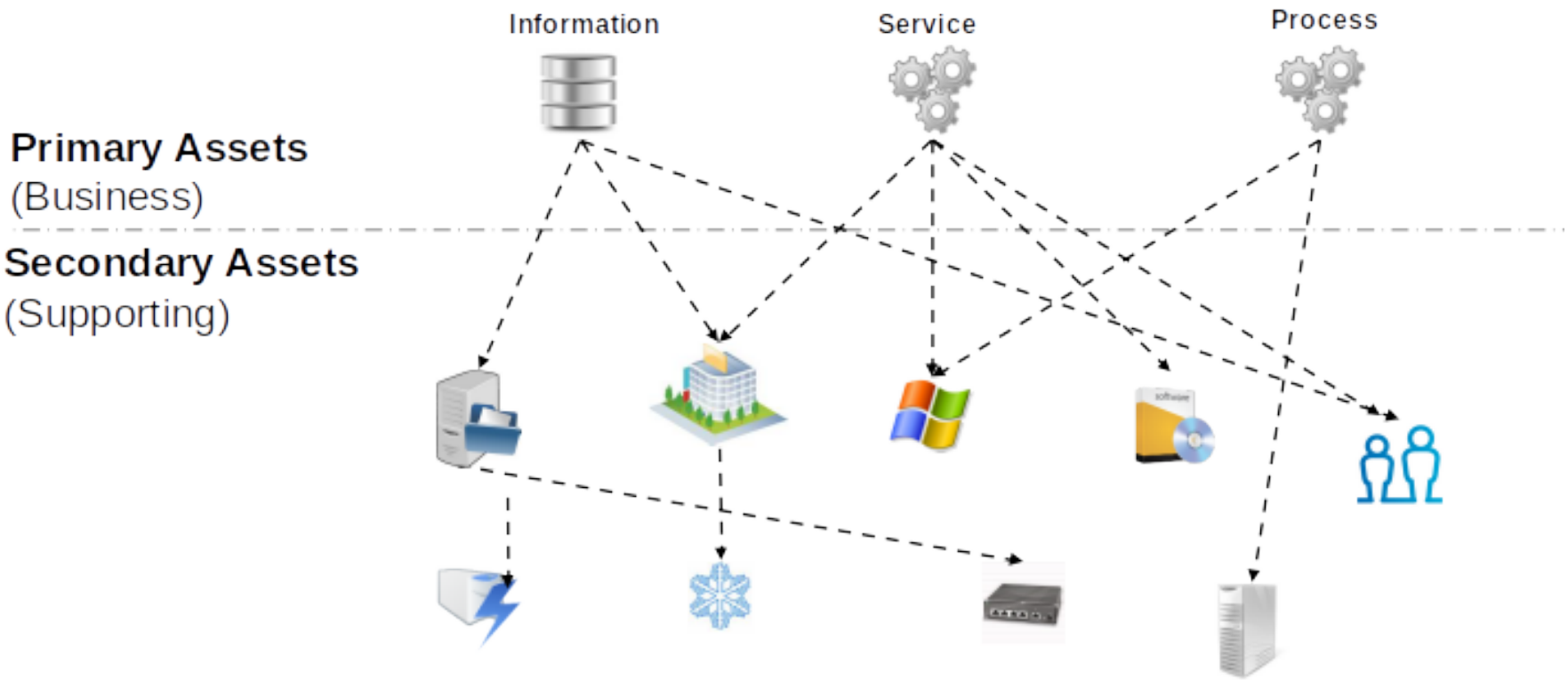
Optimizations

MONARC is an optimized method:

- inheritance on objects;
- scope of objects;
- inheritance on impacts;
- deliverables;
- multiple dashboards and reporting possibilities.

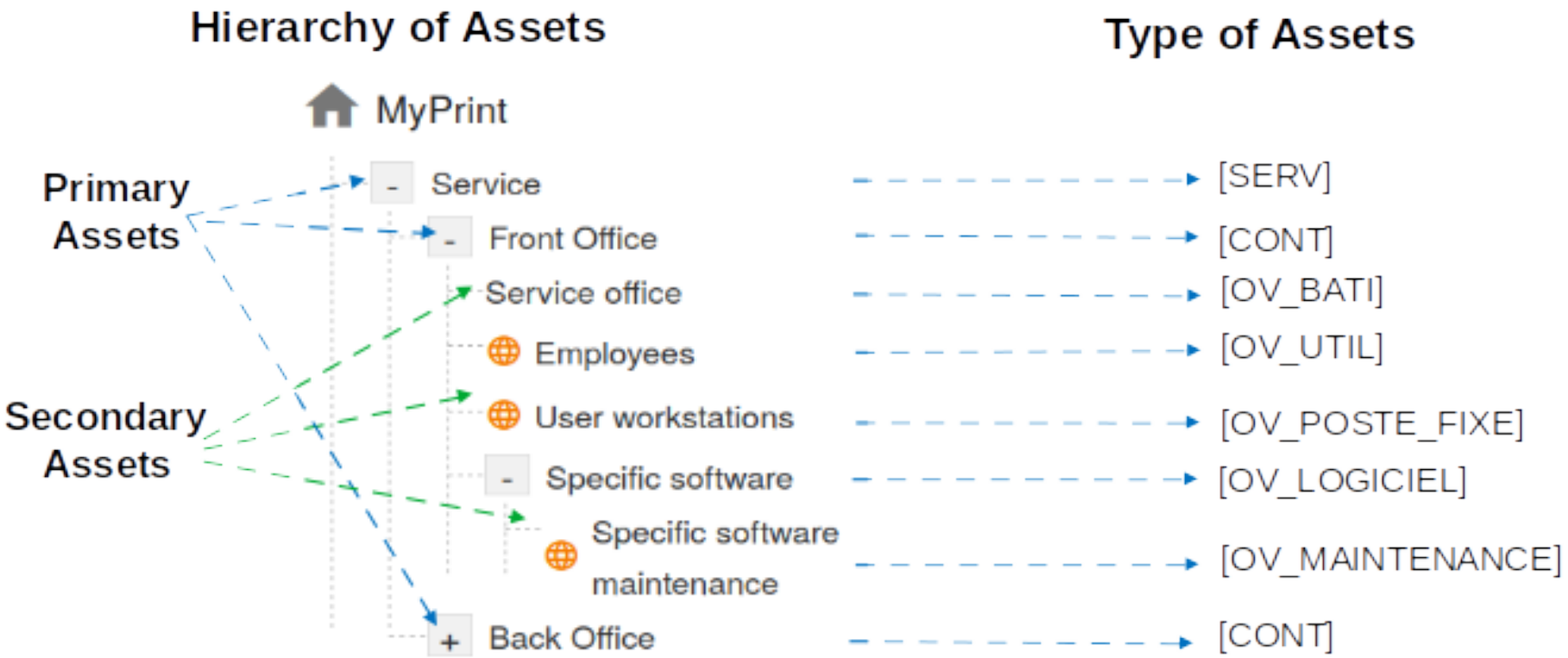
Inheritance on objects

Modelling



Inheritance

Formalisation of the modelling



Inheritance

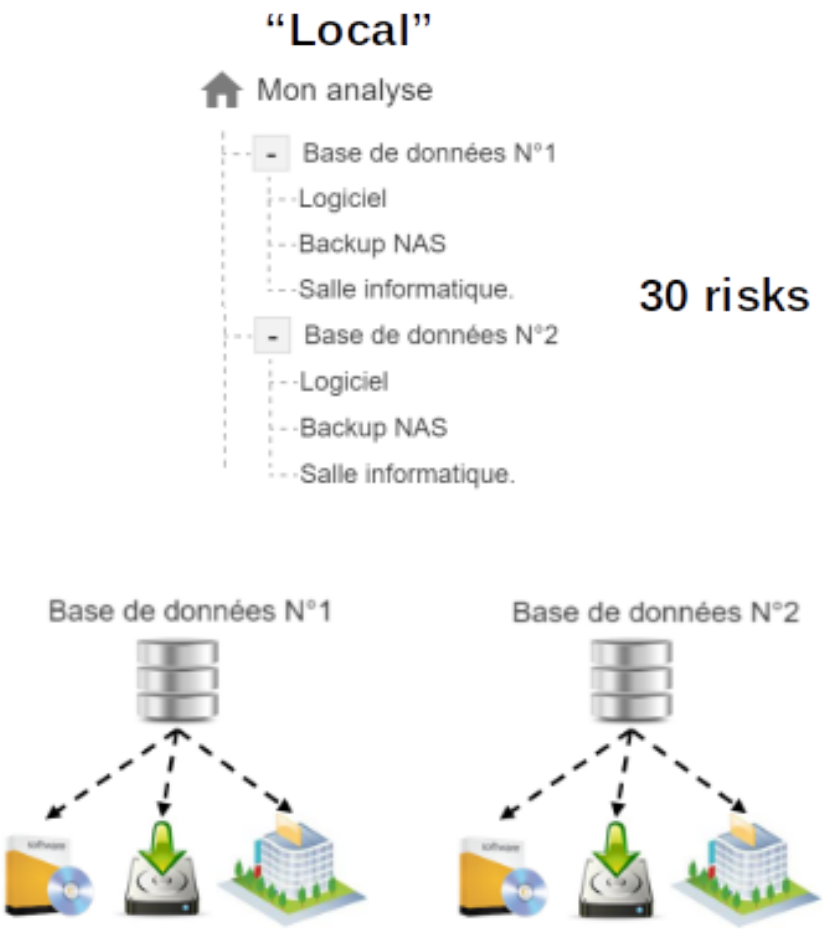
Formalisation of an asset

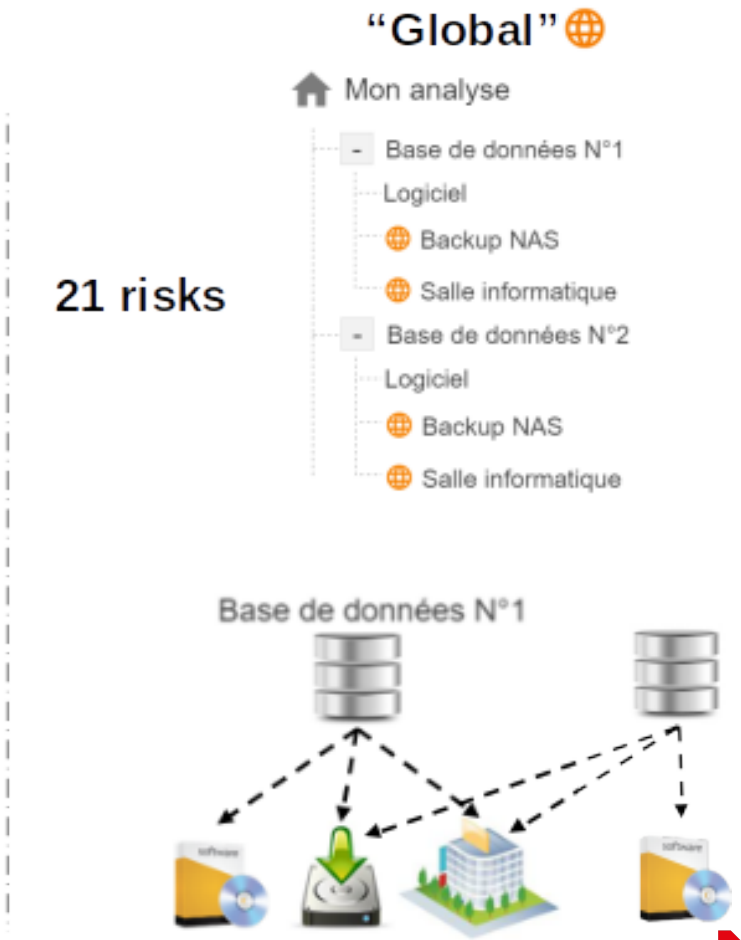
Example with `OV_BATI`

Threat	Vulnerability
Theft or destruction of media, documents or equipment	Flaws in the physical access boundaries
Theft or destruction of media, documents or equipment	The principle of least privilege is not applied
Theft or destruction of media, documents or equipment	Authorisation management is flawed
Abuse of rights	No supervision of third-party access (supplier, cleaner, etc.)
Environmental disaster (fire, flood, dust, dirt, etc.)	Premises are not secure or could be compromised by external elements

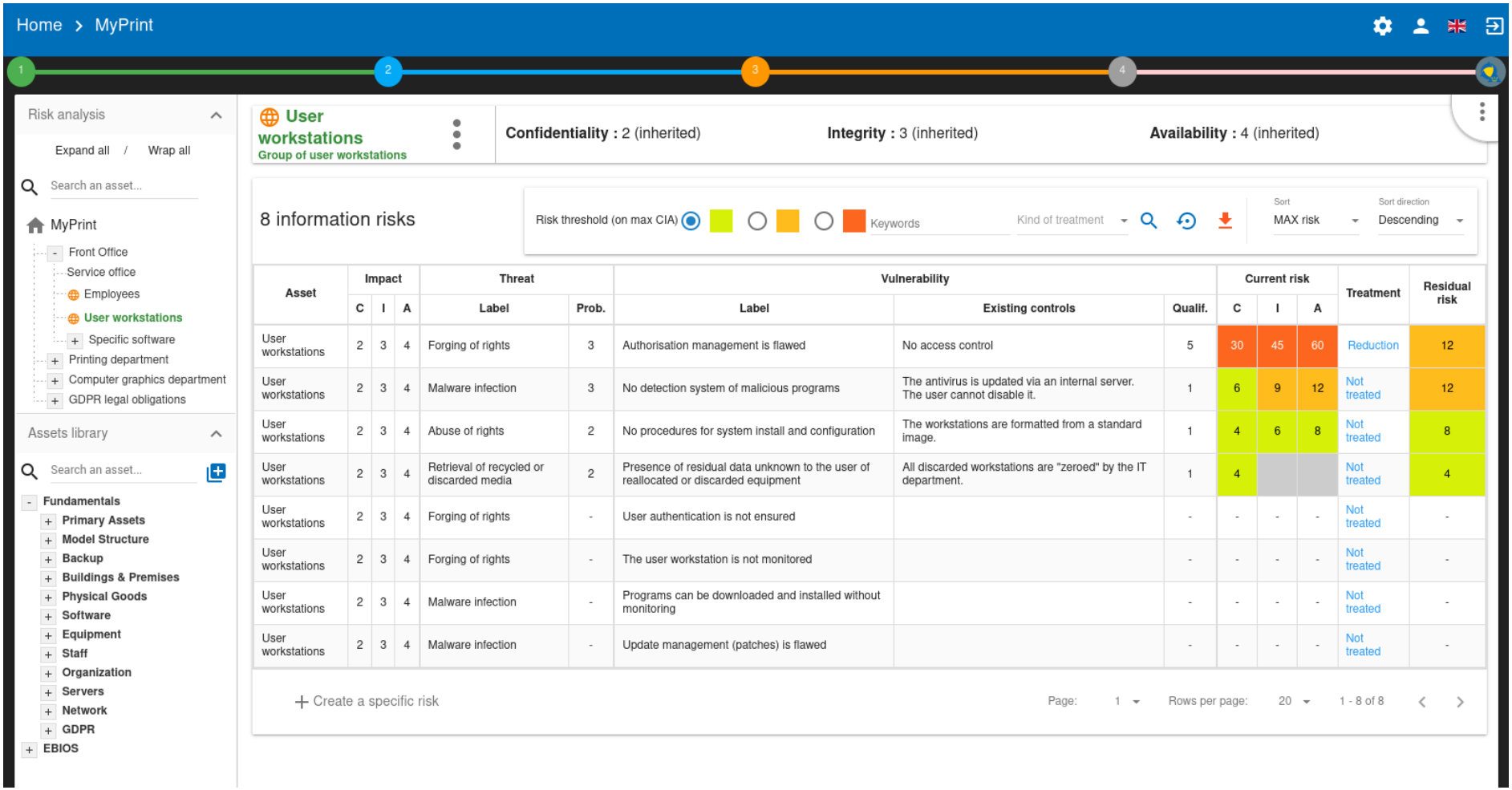
Scope of objects

Global or local assets





Inheritance on impacts

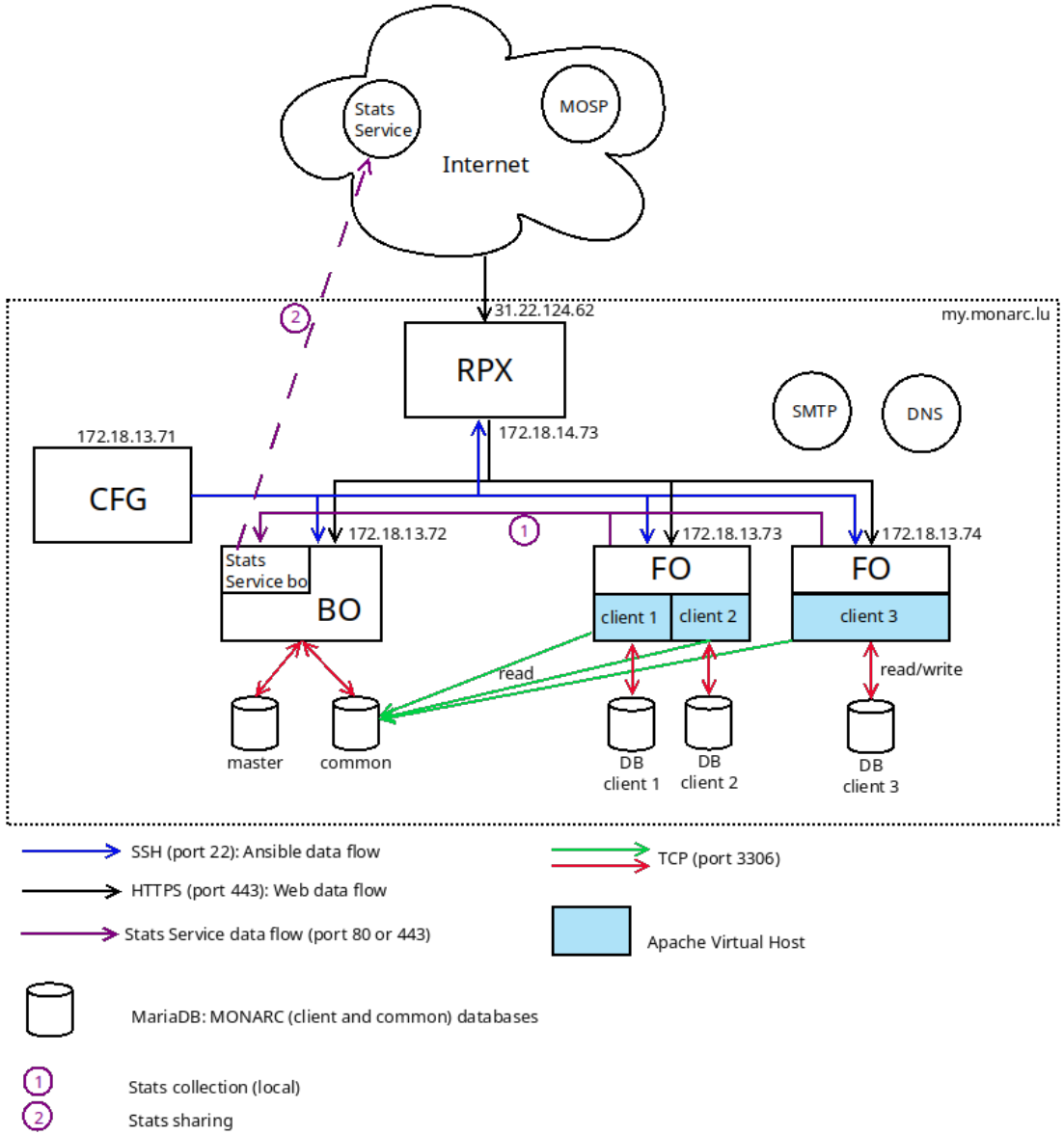


Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
User workstations	2	3	4	Forging of rights	3	Authorisation management is flawed	No access control	5	30	45	60	Reduction	12
User workstations	2	3	4	Malware infection	3	No detection system of malicious programs	The antivirus is updated via an internal server. The user cannot disable it.	1	6	9	12	Not treated	12
User workstations	2	3	4	Abuse of rights	2	No procedures for system install and configuration	The workstations are formatted from a standard image.	1	4	6	8	Not treated	8
User workstations	2	3	4	Retrieval of recycled or discarded media	2	Presence of residual data unknown to the user of reallocated or discarded equipment	All discarded workstations are "zeroed" by the IT department.	1	4			Not treated	4
User workstations	2	3	4	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
User workstations	2	3	4	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-
User workstations	2	3	4	Malware infection	-	Programs can be downloaded and installed without monitoring		-	-	-	-	Not treated	-
User workstations	2	3	4	Malware infection	-	Update management (patches) is flawed		-	-	-	-	Not treated	-

Deliverables

Shareable and customised templates of deliverables.

Summary



MOSP: https://objects.monarc.lu
Stats Service: https://dashboard.monarc.lu
Stats Service bo: internal Stats Service instance, for example dashboard.my.monarc.lu

Le’ts work a little!

- connect to the MONARC formation instance: `https://formation.monarc.lu`
- use the provided login (`user_XY@monarc.lu`) and the password `Password1234!`

Compatible Web browsers: Firefox, Chrome and Safari.

Dashboard

- provide different visualizations of the current analysis state;
- visualizations are exportable (.png, .csv, .pptx).

Statement of Applicabitity

Statement of Applicability (SOA) and compliance level for a referential security.

Record of processing activities

Register of the information treatment for processing activities.

Latest notable developments

- PHP 8 compatibility, possibility to link multiple specific models per client, new feature to enforce two-factor authentication. (MONARC 2.12.6);
- two-factor authentication, compliance scale, metadata assets (MONARC 2.12.1);
- definition of custom scales for operational risks (MONARC 2.11.0);
- dashboard for the CEO with data gathered from different MONARC instances (MONARC 2.10.1);
- records of processing activities for the GDPR and set of recommendations (MONARC 2.9.0);
- connection with MOSP (MONARC 2.8.2);
- statement of applicability (MONARC 2.7.0).

Future developments

- management of dependencies between services;
- enhancements to the global dashboard towards a security weather forecast[2];
- enhancements to the sharing of MONARC objects with MOSP[3];
- import of models in back office;
- link between GDPR module and some objects in MONARC.

Idea ? $\rightarrow$ Discussions on GitHub

[2] https://dashboard.monarc.lu
[3] https://objects.monarc.lu

Services related to MONARC

- help at deploying;
- help at using;
- trainings;
- developments, feature requests.

End of the presentation

- Thank you for listening.
- Contact: opensource@nc3.lu
- `https://github.com/NC3-LU`
- `https://github.com/monarc-project`
- `https://www.monarc.lu`