Introduction to MONARC

Optimised Risk Analysis Method

Security Made In Lëtzebuerg / CASES

Cyberworld Awareness and Security Enhancements Services

December 03, 2020

cases.lu
Cyberworld Awareness and
Security Enhancement Services
LUXEMBOURG

Security Made In Lëtzebuerg

Our timeline

- 2003: Cyberworld Awareness and Security Enhancements Services (**CASES**);
- 2007: Computer Incident Response Center Luxembourg (**CIRCL**);
- 2010: Security Made In Lëtzebuerg is a *GIE* (Groupement d'Intérêt Économique);
- 2017: Cyber security Competence Center (**C3**).

CASES

Mission

Promote information security by supporting Luxembourg administrations and SMEs.

Services:

- **awareness**: article publications;
- **trainings**: introduction to cyber security for different audiences [1];
- **software**: MONARC, MOSP, Fit4Cybersecurity, Fit4Contract, Fit4Gdpr (coming soon), TACOS, etc.[2]

Cooperation with ANSSI-LU (National Cybersecurity Agency of Luxembourg), CCB (Centre for Cyber security Belgium) and others.

[1] https://www.cases.lu/services/trainings.html

[2] https://github.com/CASES-LU

Content at glance

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

Summary

An open source software

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

For many users, it started with a spreadsheet.

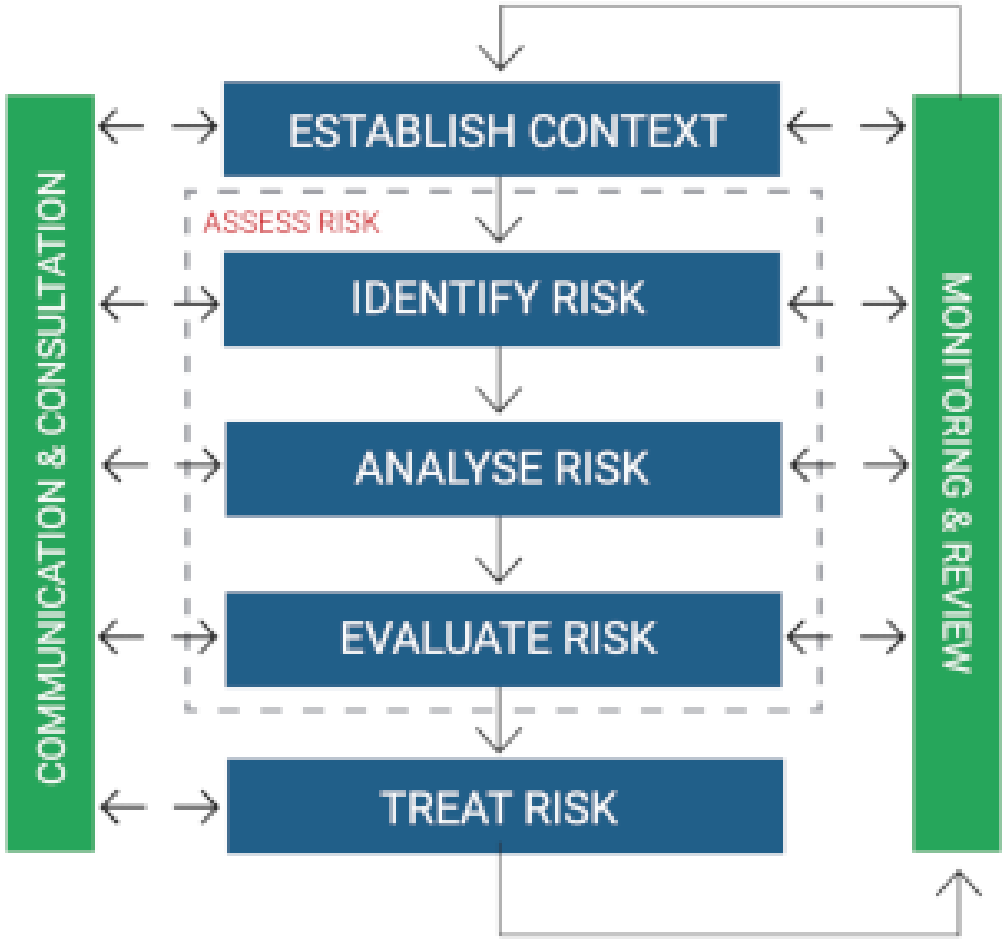
[3] `https://github.com/monarc-project`

A community

- more than 190 organizations:
  `https://my.monarc.lu`;
- sharing MONARC objects (threats, assets, recommendations, etc.):
  `https://objects.monarc.lu`;
- a future global dashboard with trends about threats and vulnerabilitties:
  `https://dashboard.monarc.lu`.

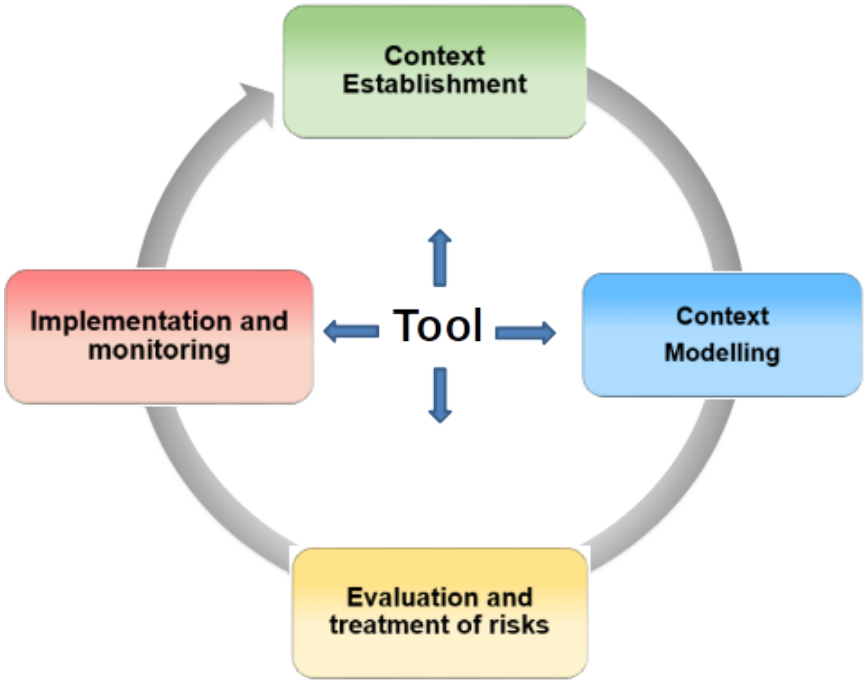
A method

Based on ISO/IEC 27005:2011, but optimized



Summary

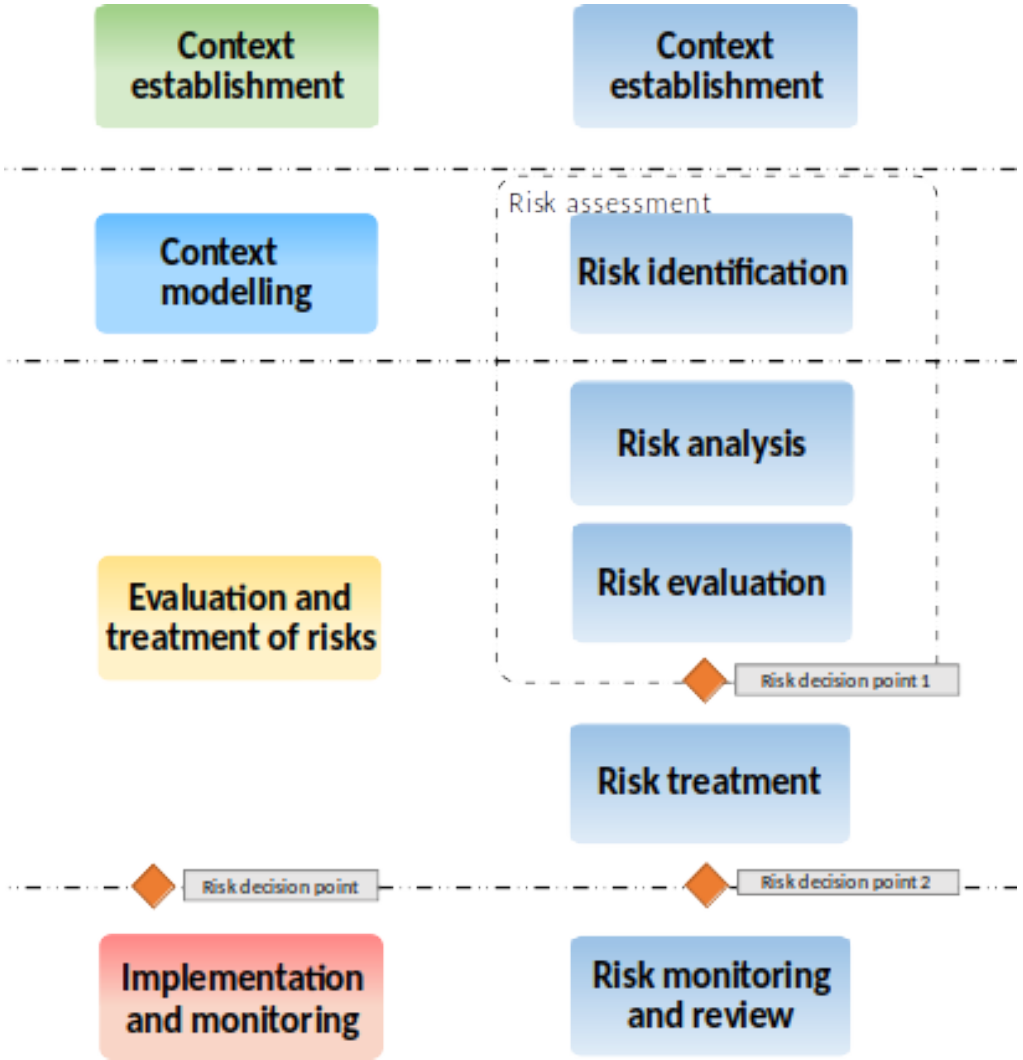
A Structured, Iterative and Qualitative method



- 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).

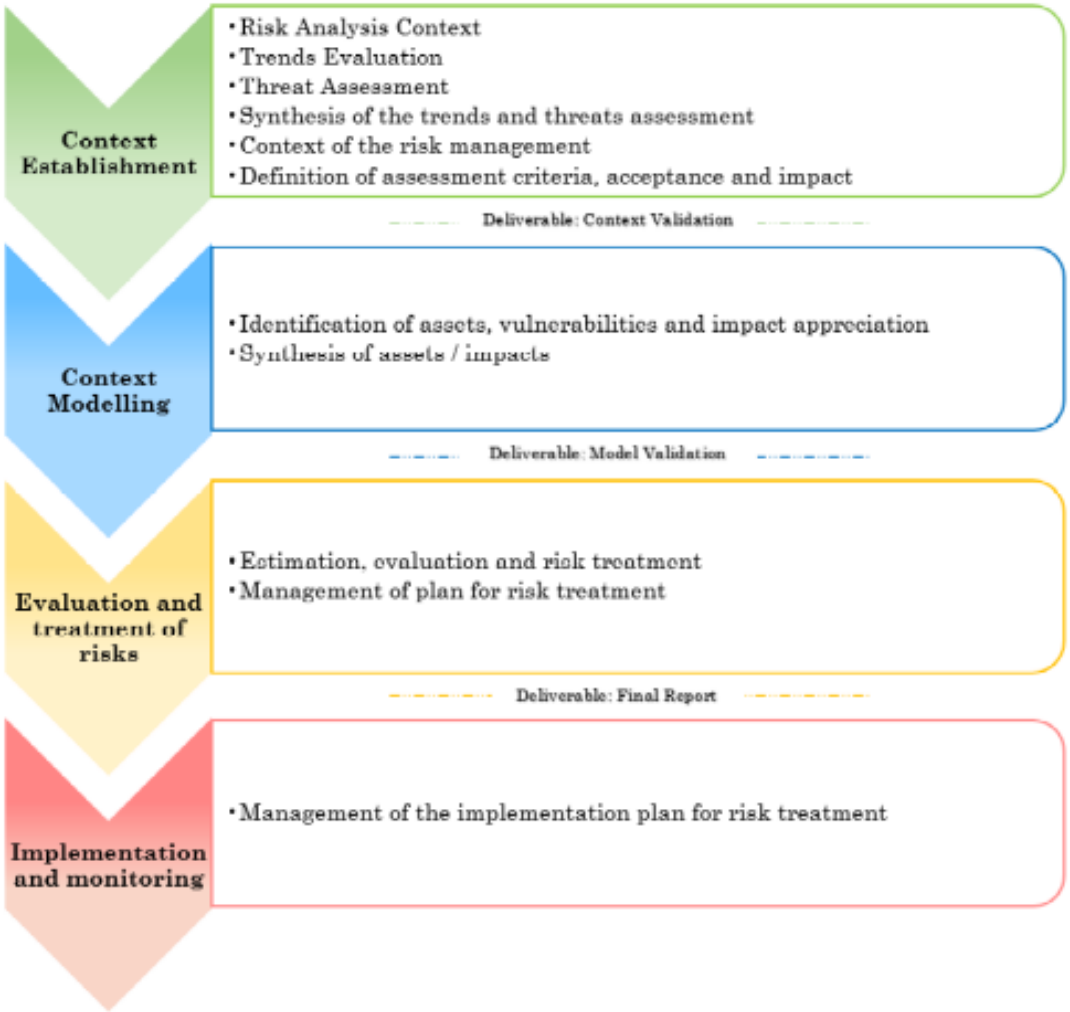
Automated and simplified management

Method based on ISO/IEC 27005



Automated and simplified management

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



ISO/IEC 27005:2011

Information risks

Formula

$$R = I \times T \times V$$

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

ISO/IEC 27005:2011

Operational risks

Formula

$$R = I \times P$$

- impact on ROLFP;
- on primary assets.

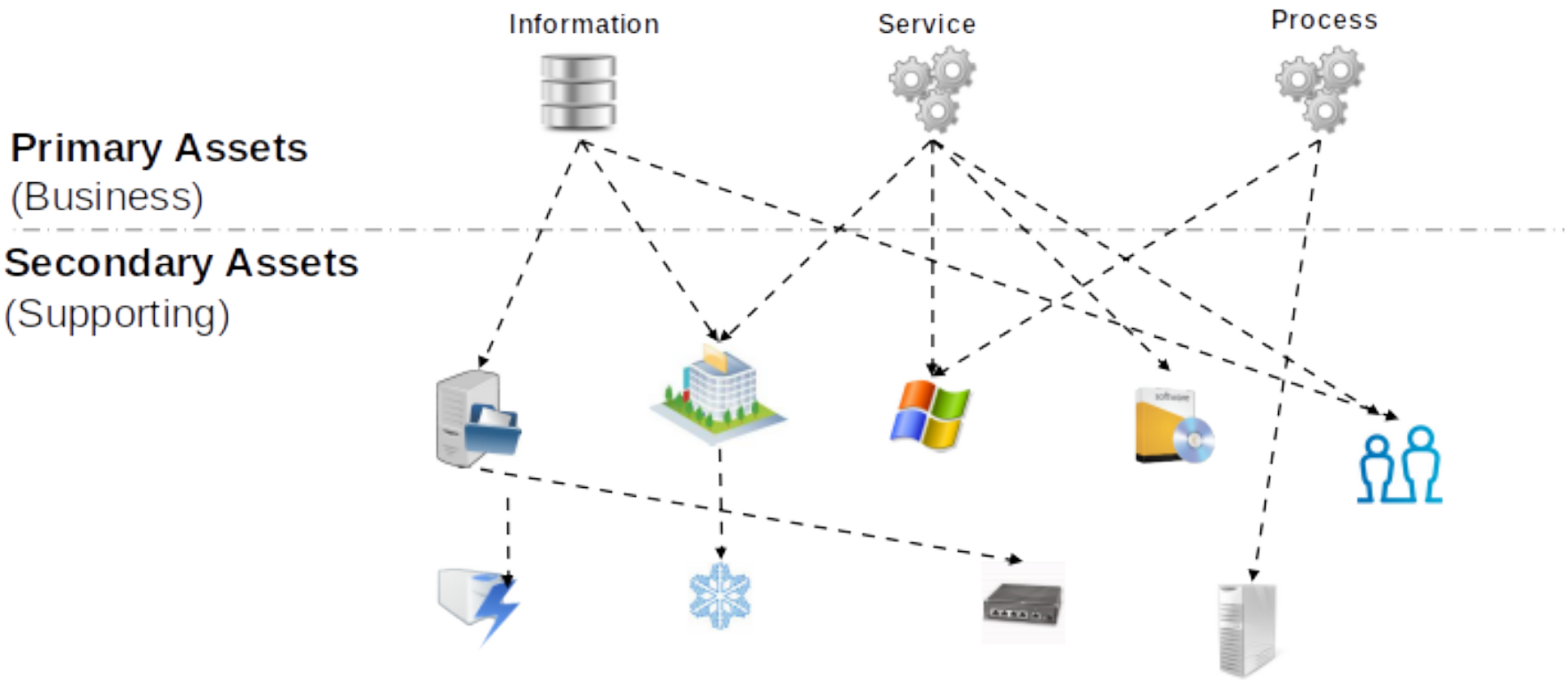
Optimizations

MONARC is an optimized method:

- inheritance on objects;
- scope of objects;
- inheritance on impacts;
- deliverables.

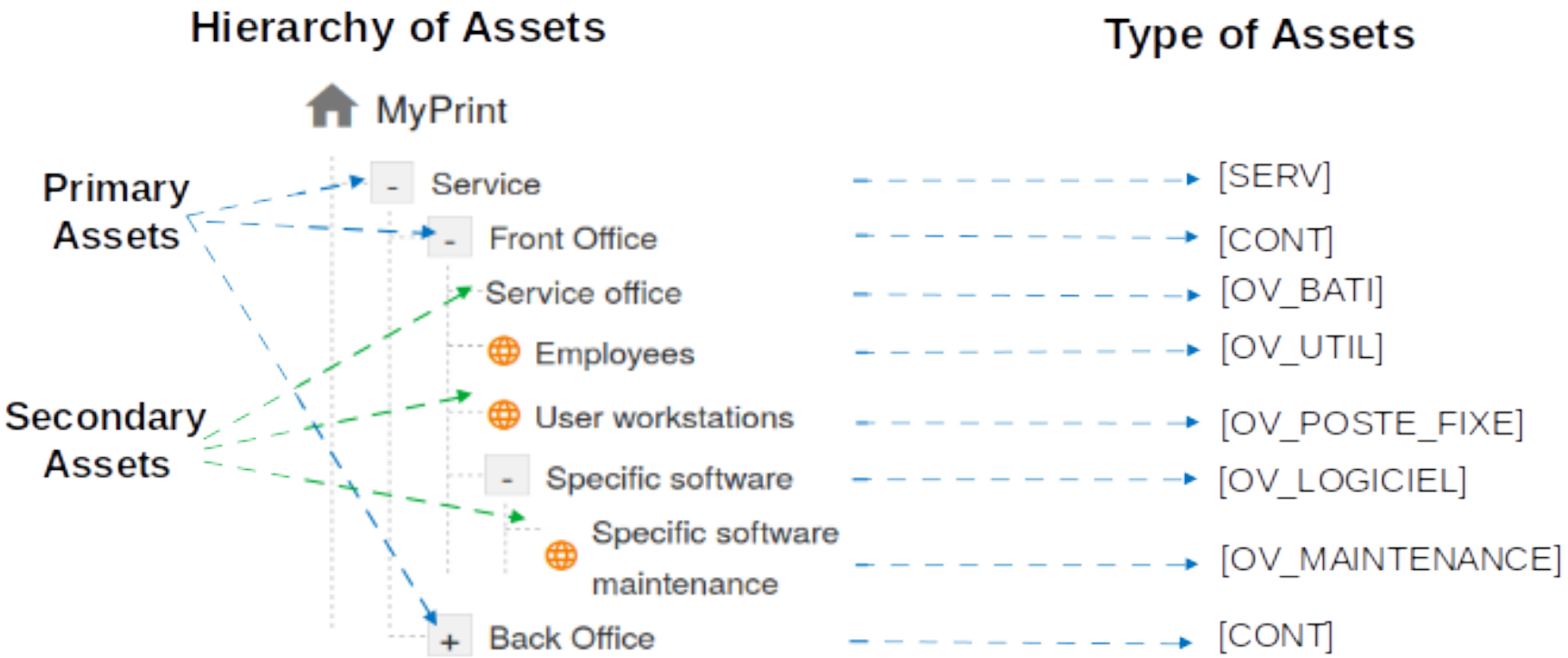
Inheritance on objects

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

"Local"

Mon analyse

- Base de données N°1
  - Logiciel
  - Backup NAS
  - Salle informatique.
- Base de données N°2
  - Logiciel
  - Backup NAS
  - Salle informatique.

30 risks

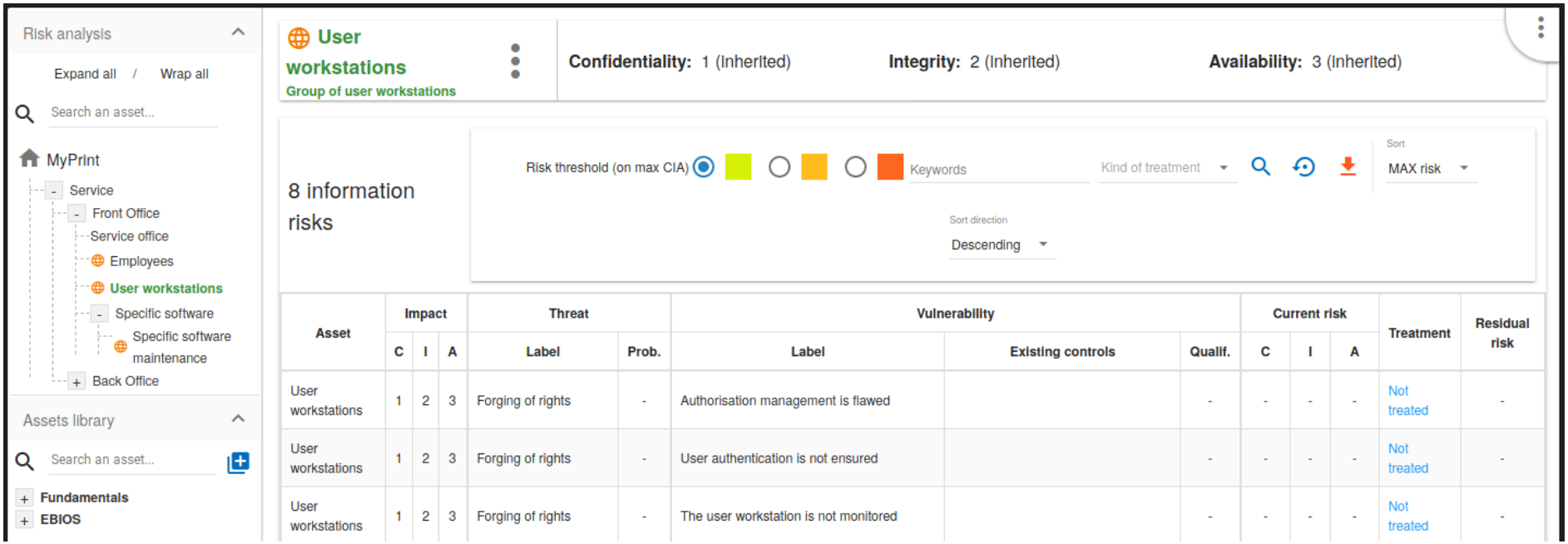
"Global"

Mon analyse

- Base de données N°1
  - Logiciel
  - Backup NAS
  - Salle informatique
- Base de données N°2
  - Logiciel
  - Backup NAS
  - Salle informatique

21 risks

Inheritance on impacts

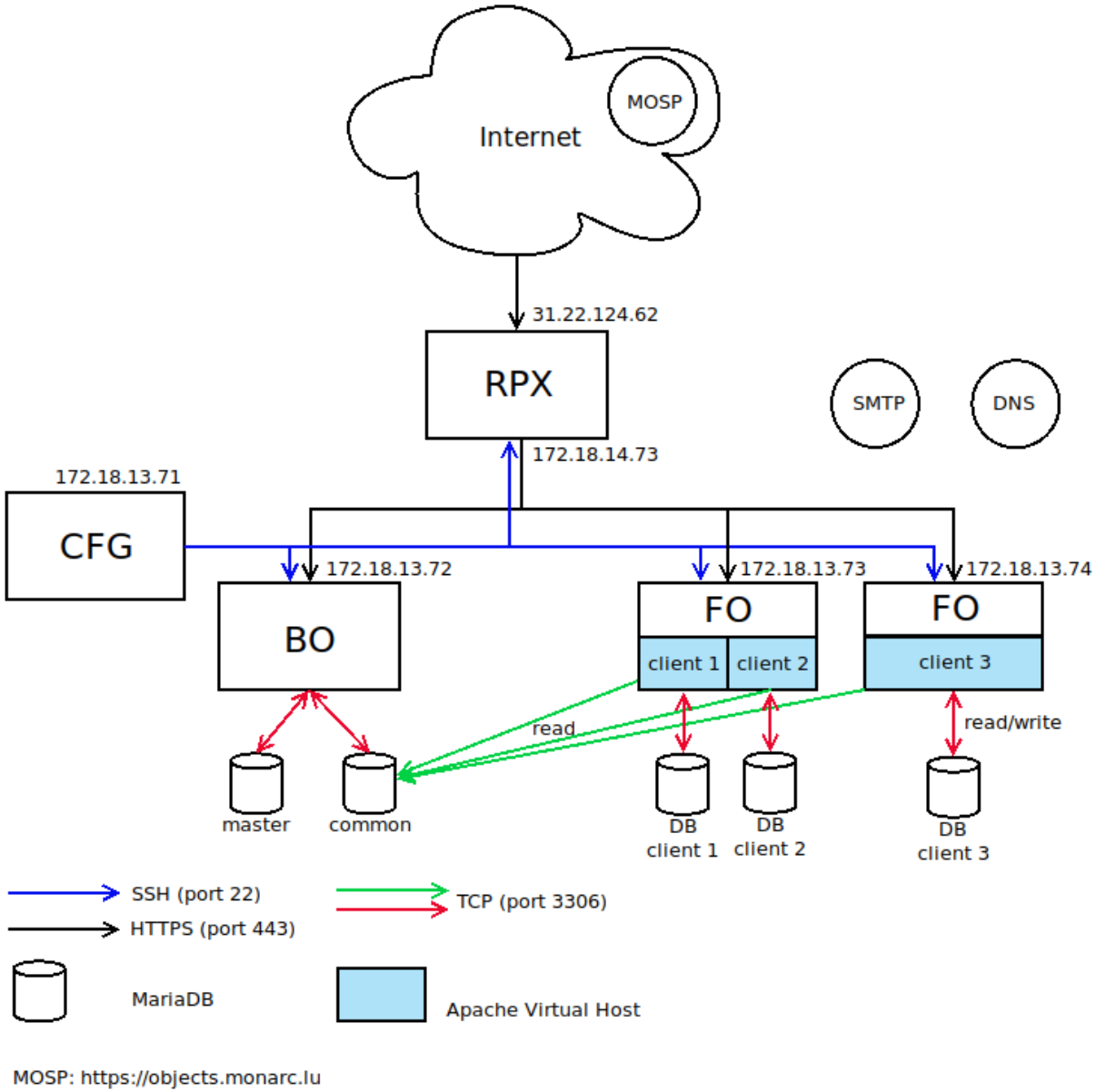


Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
User workstations	1	2	3	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not treated	-
User workstations	1	2	3	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
User workstations	1	2	3	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-

Deliverables

Shareable templates of deliverables.

Summary


Internet
MOSP
31.22.124.62
RPX
SMTP
DNS
172.18.14.73
172.18.13.71
CFG
172.18.13.72
BO
172.18.13.73
FO
client 1
client 2
172.18.13.74
FO
client 3
read
read/write
master
common
DB
client 1
DB
client 2
DB
client 3
SSH (port 22)
HTTPS (port 443)
TCP (port 3306)
MariaDB
Apache Virtual Host
MOSP: https://objects.monarc.lu

Le'ts work a little!

- training instance: `https://formation.monarc.lu`
- login: `user_X@monarc.lu`, where $01 \leq X \leq 30$;
- password: `Password1234!`

Preferably use Firefox, alternatively Chrome. But not Internet Explorer.

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

- statement of applicability (MONARC 2.7.0);
- connection with MOSP (MONARC 2.8.2);
- records of processing activities for the GDPR (MONARC 2.9.0);
- management of set of recommendations (MONARC 2.9.0);
- port of the backend to Zend Framework 3 (MONARC 2.9.1);
- new dashboard for the CEO role: global dashboard with data gathered from different MONARC instances. (MONARC 2.10.1).

Future developments

- improvements of the new global dashboard towards a security weather forecast;
- enhancements to the sharing of MONARC objects (via MOSP[4]);
- link between GDPR module and some objects in MONARC;
- new front-end.

Idea ? $\rightarrow$ Feature request

[4] 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: info@cases.lu
- `https://github.com/monarc-project`
- `https://www.monarc.lu`