Introduction to MONARC

Optimised Risk Analysis Method

SECURITYMADEIN.LU / CASES

Cyberworld Awareness and Security Enhancements Services

April 19, 2022

SECURITYMADEIN.LU

Our history:

- 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);
- 2017: Cyber security Competence Center (**C3**).

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

CASES

Mission

Foster cyber security by supporting Luxembourg administrations and SMEs.

Services

- **Awareness**: publications of articles and videos;
- **Trainings**: introduction to cyber security for different audiences;
- **Software**: MONARC, MOSP, Fit4Cybersecurity, etc.

Cooperations

ANSSI-LU, Centre for Cyber Security Belgium, KonzeptAcht GmbH, ILR, GRC-Luxembourg and others.

Content at glance

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 260 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

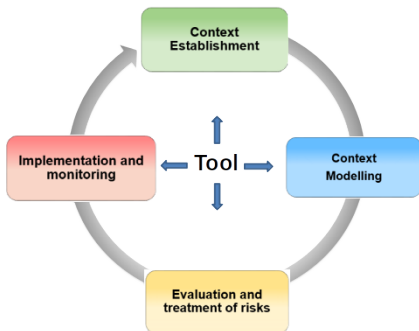Based on `ISO/IEC 27005:2011`, but optimized
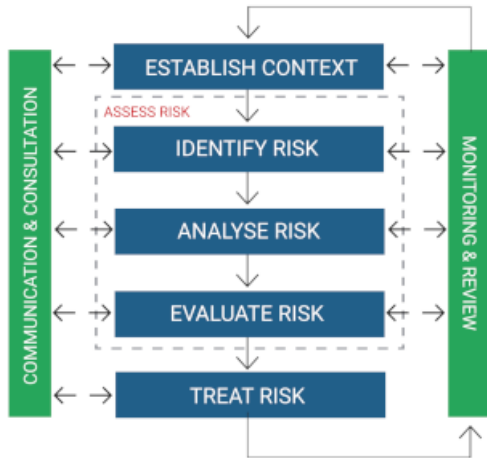
Summary

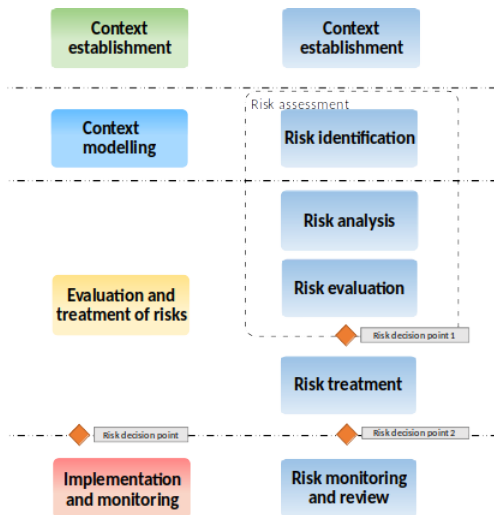# A Structured, Iterative and Qualitative method

- 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).
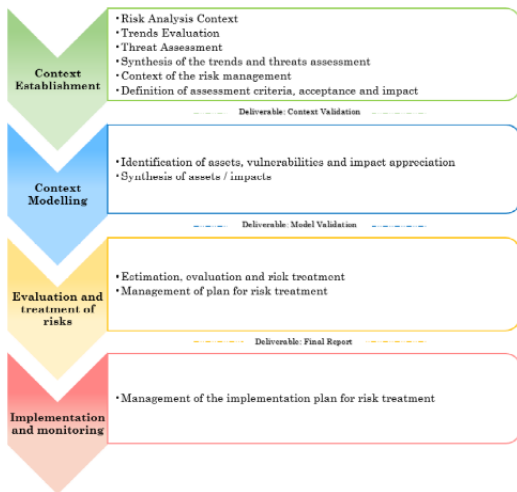
Possibility to define custom scales for operational risks.

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

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

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

Operational risks

$$R = I \times P$$

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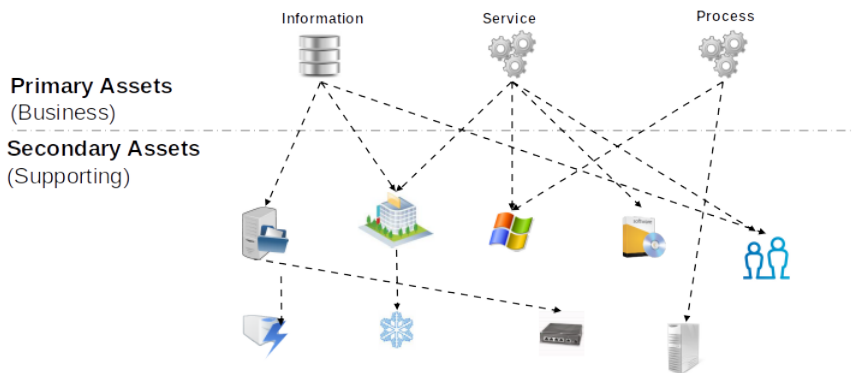- on primary assets.

Optimizations

MONARC is an optimized method:

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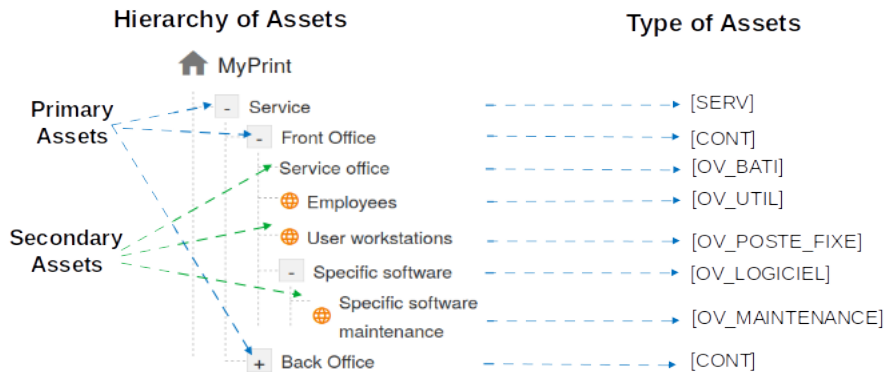- multiple dashboards and reporting possibilities.

Inheritance on objects

Modelling

Inheritance

Formalisation of the modelling

Hierarchy of Assets

Type of Assets

🏠 MyPrint

Primary Assets
- Service .... [SERV]
- Front Office .... [CONT]
  Service office .... [OV_BATI]
  🌐 Employees .... [OV_UTIL]

Secondary Assets
  🌐 User workstations .... [OV_POSTE_FIXE]
  - Specific software .... [OV_LOGICIEL]
  🌐 Specific software maintenance .... [OV_MAINTENANCE]
  + Back Office .... [CONT]

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

Deliverables

Shareable and customised templates of deliverables.

Summary

SSH (port 22): Ansible data flow

HTTPS (port 443): Web data flow

Stats Service data flow (port 80 or 443)

TCP (port 3306)

Apache Virtual Host
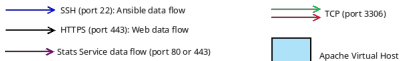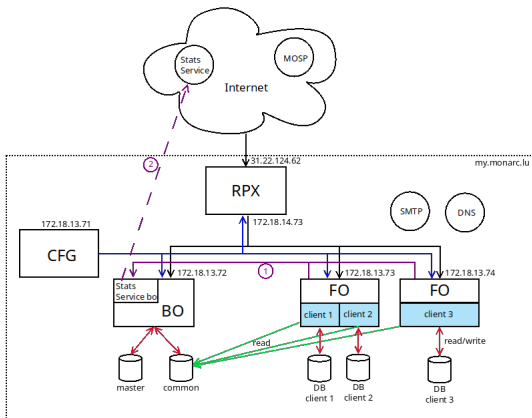
MariaDB: MONARC (client and common) databases

① Stats collection (local)

② Stats sharing

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!

- training instance: `https://formation.monarc.lu`
- login: `user_X@monarc.lu`, where $01 \leq X \leq 50$;
- password: `Password1234!`

or use the virtual machine: `https://vm.monarc.lu`

Compatible Web browsers: Firefox, Chrome and Safari.

Dashboard

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

Statement of Applicability

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

- 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

- 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;
- two-factor authentication.

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: info@cases.lu
- https://github.com/CASES-LU
- https://github.com/monarc-project
- https://www.monarc.lu