

Introduction to MONARC

Optimised Risk Analysis Method

Security Made In Lëtzebuerg / CASES

Cyberworld Awareness and Security Enhancements Services

February 12, 2020



Security Made In Lëtzebuerg (SMILE)

Our timeline

- 2003: Cyberworld Awareness and Security Enhancements Services (**CASES**);
- 2007: Computer Incident Response Center Luxembourg (**CIRCL**);
- 2010: SMILE 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, Fit4Cybersecurity, MOSP, TACOS, etc.²

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

1 What is MONARC?

- An open source software
- A community
- A method

2 The method

3 The tool



An open source software

- Web application (SaaS, self-hosted, virtual machine, etc.);
- source code³ 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

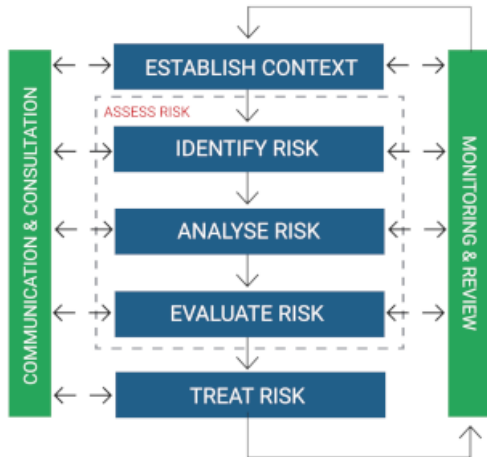
- sharing of risk models and all kind of objects (assets, threats, vulnerabilities, recommendations, referentials, etc.);
- data available via a sharing platform: MOSP⁴;
- more than 130 organizations on <https://my.monarc.lu>.

⁴<https://objects.monarc.lu/organization/MONARC>



A method

Based on ISO/IEC 27005:2011, but optimized

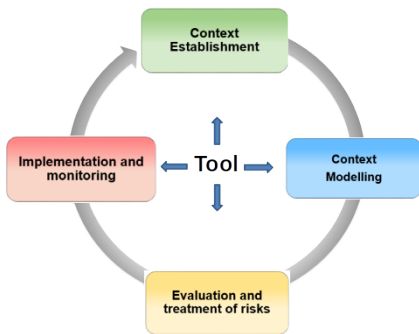


Summary

- 1 What is MONARC?
- 2 The method
 - Management of risk
 - An optimized method
- 3 The tool



A Structured, Iterative and Qualitative method

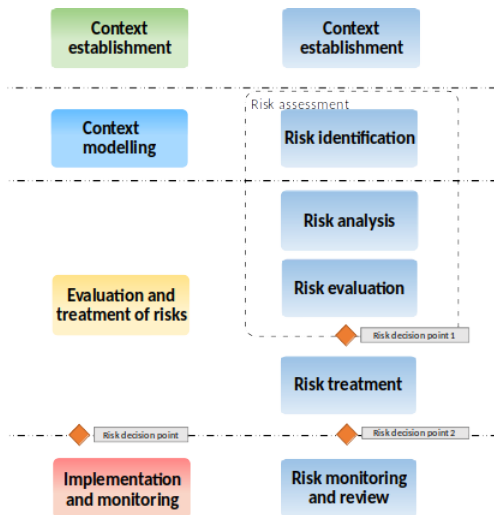


- Structured: 1, 2, ..., n.
- Iterative: **Plan, Do, Check, Act**
- Qualitative: **Values / Consequence**
 - Impact/Consequence, Threat, Vulnerability;
 - reputation, image;
 - operation;
 - legal;
 - financial;
 - person (to the).



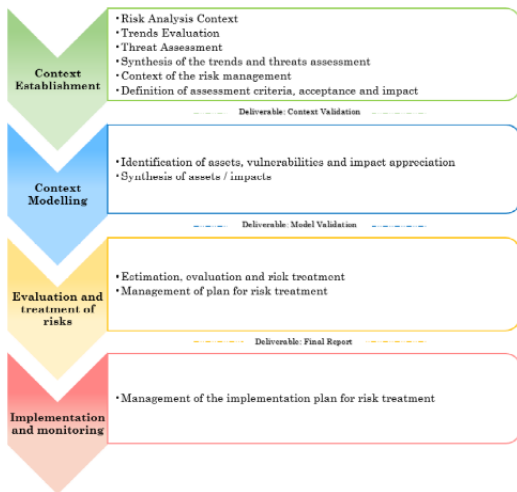
Automated and simplified management

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

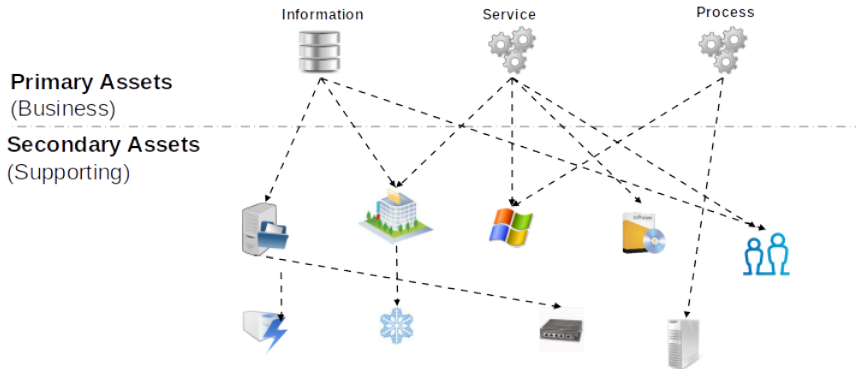
MONARC is an optimized method:

- inheritance;
- scope of objects;
- models;
- deliverables.



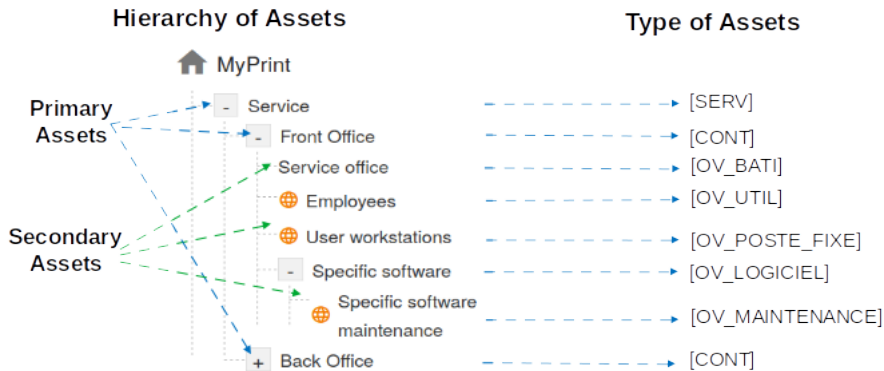
Inheritance

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

Base de données N°1



Base de données N°2



Base de données N°1



Inheritance of impacts

Risk analysis


Expand all / Wrap all

Search an asset...

MyPrint

- Service
 - Front Office
 - Service office
 - Employees
 - User workstations
 - Specific software
 - Specific software maintenance
 - Back Office




Assets library


Search an asset... 

- Fundamentals
- EBIOS

User workstations
Group of user workstations

Confidentiality: 1 (Inherited) Integrity: 2 (Inherited) Availability: 3 (Inherited)

Risk threshold (on max CIA)  Keywords Kind of treatment  Sort: MAX risk 

Sort direction: Descending 

8 information risks

| 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 | - |



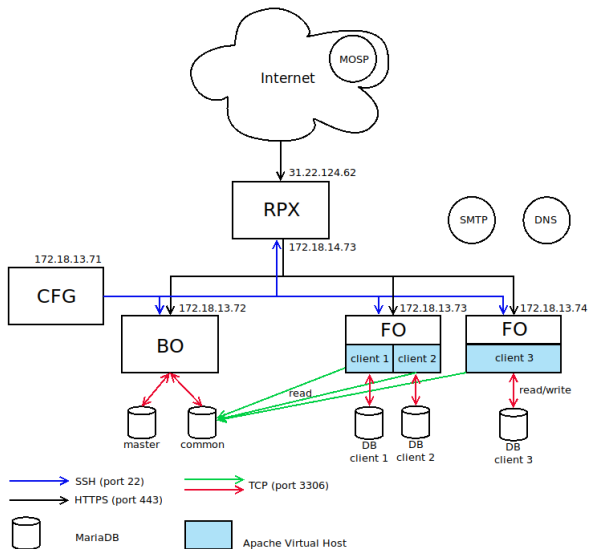
Deliverables

Shareable templates of deliverables.

Summary

- 1 What is MONARC?
- 2 The method
- 3 The tool
 - Architecture
 - Workshop
 - Modules
 - Roadmap





MOSP: <https://objects.monarc.lu>



Le'ts work a little!

- **training instance:** `https://formation.monarc.lu;`
- **login:** `user_en_X@monarc.lu`, where $01 \leq X \leq 15$;
- **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 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

- port of the backend to Zend Framework 3 (MONARC 2.9.1);
- records of processing activities for the GDPR (MONARC 2.9.0);
- management of set of recommendations (MONARC 2.9.0);
- connection with MOSP (MONARC 2.8.2);
- statement of applicability (MONARC 2.7.0).



Future developments

- LDAP;
- single sign-on;
- improvements of the dashboard towards a security weather forecast;
- enhancements to the sharing of MONARC objects (via MOSP⁵);
- link between GDPR module and some objects in MONARC;
- new front-end.

Idea → Feature request

⁵<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>

