WORKSHOP MONARC
(OPTIMISED RISK ANALYSIS METHOD)

MONARC V2.0 TRAINING
INFO@CASES.LU
Legal Form: G.I.E (Groupement d’Intérêt Economique)

www.securitymadein.lu
www.cases.lu
AGENDA

- What is MONARC?
- Discovery and usage of the tool
- Run-through of the method
- Tips & Tricks
Risk Analysis Method

- Structured
  1. ...
  2. ...
  n. ...

- Iterative
  - Plan
  - Do
  - Check
  - Act

- Qualitative: Values / consequences
  - Reputation, Image
  - Operation
  - Legal
  - Financial
  - Person (to the)
  - ...

Tool

Context Establishment

Implementation and monitoring

Evaluation and treatment of risks

Context Modelling

MONARC: OPTIMISED RISK ANALYSIS METHOD
MONARC : À RETENIR

- **Open source**
  
  www.github.com/CASES-LU/MonarcAppFO
  
  AGPL v3.0 (GNU Affero General Public License version 3)

- **Risk Management**
  
  Information Risks ($R = I \times M \times V$)
  
  - Impact on the CIA
  
  Secondary Assets

  Operational Risks ($R = I \times P$)
  
  - Impact on the ROLFP
  
  Gross/Net
  
  Primary Assets

- **Sharing of Risk Models**

- **Optimised** (models, delivrables, inheritance, globalisation)
AGENDA

- What is MONARC?
- Discovery and usage of the tool
- Run-through of the method
- Tips & Tricks
MAIN FEATURES/FUNCTIONALITIES

Démonstration
AGENDA

- What is MONARC?
- Discovery and usage of the tool
- Run-through of the method
- Tips & Tricks
MONARC : LA MÉTHODE EN DÉTAILS

- **Context Establishment**
  - Risk Analysis Context
  - Trends Evaluation
  - Threat Assessment
  - Synthesis of the trends and threats assessment
  - Context of the risk management
  - Definition of assessment criteria, acceptance and impact
  - Deliverable: Context Validation

- **Context Modelling**
  - Identification of assets, vulnerabilities and impact appreciation
  - Synthesis of assets / impacts
  - Deliverable: Model Validation

- **Evaluation and treatment of risks**
  - Estimation, evaluation and risk treatment
  - Management of plan for risk treatment
  - Deliverable: Final Report

- **Implementation and monitoring**
  - Management of the implementation plan for risk treatment
1.1 – CONTEXT OF THE RISK ANALYSIS

- Discovering the target organisation
- Links with ISO 27005:2011
  - General considerations: Chapter 7.1
  - Risk Management Approach: Chapter 7.2.1
  - Basic Criteria: Chapters 7.2.2, 7.2.3, 7.2.4
  - Targets and Limits: Chapter 7.3
1.2 – EVALUATION OF TRENDS

- Kick-off meeting: Key people (management, team coordinators, IT, Quality, …)
- Broad/general questions to identify the context
- Define the scope and focus of the analysis
- Information collection
1.2 – EVALUATION OF THREATS

- Go through some Threats, involve the group, define the context
- Collect information before individual interviews
1.2 – SUMMARY

- Summarise the important information collected during the evaluation of trends and threats.
- This information will complete the first deliverable.
1.3 – ORGANISATION OF THE RISK MANAGEMENT

- Additional information on risk management within the organisation
- Links with ISO 27005:2011
  - Organisation of risk management: Chapter 7.4
1.4 – DEFINITION OF EVALUATION, ACCEPTANCE AND IMPACT CRITERIA

Acceptance thresholds of information risks

<table>
<thead>
<tr>
<th>Impact</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Acceptance thresholds of operational risks

<table>
<thead>
<tr>
<th>Impact</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Impacts scale: [0 - 4]

0  Nonexistent impact. The confidentiality criterion is not important.
1  Weak impact, insignificant.
   Information leaks are negative to the organization’s interests.
   Examples: - Internal information leaks which shouldn’t be outside the company.
             - Memorandum - Internal phone directory

2  Average impact, acceptable.
   Information leaks harm organization’s interests.
   Examples: - Moderately sensitive information leaks which are only for a group of people.
            - Weak impact, insignificant.

3  Average impact, unacceptable.
   Information leaks harm organization’s interests.
   Examples: - Average impact, unacceptable.

Vulnerabilities scale: [0 - 5]

0  No vulnerabilities.
1  Very weak vulnerability: Some efficient measures have been already taken, and their effectiveness is controlled.
2  Weak vulnerability: Some efficient measures have been already taken.
3  Average vulnerability: Some measures have been already taken, even though they could be better.
4  Strong vulnerability: Some measures have been already taken, even though they are ineffective or unadapted.
5  Very strong vulnerability: No measures have been implemented.

Link with ISO 27005:2011
- Organisation of risk management: Chapter 7.2.2, 7.2.3, 7.2.4
1.5 – DELIVERABLE: CONTEXT VALIDATION

- Compile all the information collected during the context establishment
- Report is used to validate the collected information before the identification of risks starts.
- Export format: Microsoft Word
The combination of risks of an supporting asset is transmitted to the business asset through inheritance of the CIA evaluation.
FORMALISATION OF THE MODELLING

Hierarchy of Assets

- **Primary Assets**
  - Service
    - Front Office
    - Bureau du service
    - Employés
    - Postes de travail utilisateurs
    - Logiciel
    - Maintenance logiciel

- **Secondary Assets**

**Type of Assets**

- [SERV]
- [CONT]
- [OV_BATI]
- [OV_UTIL]
- [OV_POSTE_FIXE]
- [OV_LOGICIEL]
- [OV_MAINTENANCE]

---

<table>
<thead>
<tr>
<th>Menace</th>
<th>Vulnérabilité</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vol ou destruction de supports, de documents ou de matériel</td>
<td>Failles dans les périmètres d'accès physiques</td>
</tr>
<tr>
<td>Vol ou destruction de supports, de documents ou de matériel</td>
<td>Le principe du moindre privilège n'est pas appliqué</td>
</tr>
<tr>
<td>Vol ou destruction de supports, de documents ou de matériel</td>
<td>La gestion des autorisations comporte des failles</td>
</tr>
<tr>
<td>Abus de droits</td>
<td>Absence de vigilance lors d'une intervention d'un tiers (fournisseur, femme de ménage, etc.)</td>
</tr>
<tr>
<td>Sinistre environnemental (Incendie, eau, poussière, saleté, etc.)</td>
<td>Les locaux ne sont pas sécurisés ou peuvent être compromis par des éléments externes</td>
</tr>
</tbody>
</table>
**« GLOBAL » OR « LOCAL » ASSET**

**“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
CASES MODELLING

- Service
  - Front Office
    - Bureau du service
    - Employés
    - Postes de travail utilisateurs
    - Logiciel spécifique
      - Maintenance logiciel spécifique
  - Back Office
    - Bâtiment
    - Salle informatique
    - Administrateur système
    - Postes de travail admin
    - Gestion serveurs
    - Gestion des backups
    - Réseau & télécom
    - Organisation informatique
    - Développements logiciels

Front-Office

Back-Office
2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND IMPACTS

- Main view of MONARC
  - Creation of a risk model
- Link with ISO 27005:2011
  - Identification of assets: Chapitre 8.2.2
  - Identification of vulnerabilities: Chapitre 8.2.5
2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND IMPACTS

- Main view of MONARC
- Identification of impacts and consequences
- Link with ISO 27005:2011
- Identification of Impacts: Chapter 8.3.2
2.2 – SYNTHESIS OF ASSETS / IMPACTS

- Content justifying the choice of assets and impacts
- Designed to complete the deliverable
Contains the important, primary assets of the model (impact criteria defined)
Contains the synthesis of assets and impacts
Export format: Microsoft Word
3.1 – ESTIMATION, EVALUATION AND RISK TRAITEMENT

- Main View of MONARC
- Evaluation of some information risks.

DEMO
3.1 – ESTIMATION, EVALUATION AND RISK TREATMENT

- Main View of MONARC
- Evaluation of some operational risks
3.1 – ESTIMATION, EVALUATION AND RISK TREATMENT

- List of risks
- Creation of recommendations
3.2 – MANAGEMENT OF PLAN FOR RISK TREATMENT

- List of all the risks that have a recommendation
- Both: information risks and operational risks
3.3 – DELIVERABLE: FINAL REPORT

- Complete list of all the collected information
- Possibility to add a summary for the analysis.
- Export format: Microsoft Word
4.1 – MANAGEMENT OF THE IMPLEMENTATION PLAN FOR RISK TREATMENT

- Delegate a person in charge and fix deadlines for the implementation of each recommendation
- Validation risk by risk of their state change
- Change the value of the risk: the target risk becomes the actual risk
**4.1 – MANAGEMENT OF THE IMPLEMENTATION PLAN FOR RISK TREATMENT**

- Delegate a person in charge and fix deadlines for the implementation of each recommendation
- Validation risk by risk of their state change
- Change the value of the risk: the target risk becomes the actual risk

---

### Risk Analysis

#### Asset: Backup Management

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Existing Controls</th>
<th>Current Risk</th>
<th>New Controls</th>
<th>Target Risk</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA16 - Equipment failure</td>
<td>1174 - Backups are not carried out in accordance with the state of the art</td>
<td></td>
<td></td>
<td>48</td>
<td>24</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AGENDA

- What is MONARC?
- Discovery and usage of the tool
- Run-through of the method
- Tips & Tricks
1. Creation of an asset type
2. Creation of a threat
3. Creation of a vulnerability
4. Link assets, threats and vulnerability
5. Creation of an asset in the library
6. Use of an asset in the analysis
T&T: IMPORT / EXPORT ASSETS

- Possibility to import and export assets:
  - From/into the library
  - From/into the analysis – with or without the evaluation.