



**CASES**  
LUXEMBOURG

# **MONARC**

## **Optimised Risk Analysis Method**

# **Quick Start**

## **v1.0**

## Table of contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
1.1	PURPOSE OF THE DOCUMENT .....	3
1.2	OTHER DOCUMENTS .....	3
1.3	COMPATIBILITY WARNING .....	3
1.4	SYNTAX USED IN THE DOCUMENT .....	3
1.5	SYNTAX USED IN MONARC .....	3
<b>2</b>	<b>HOME PAGE.....</b>	<b>4</b>
2.1	FIRST CONNECTION SCREEN .....	4
2.2	CREATING THE FIRST RISK ANALYSIS.....	4
2.3	DESCRIPTION OF THE MAIN VIEW .....	5
<b>3</b>	<b>SIMPLIFIED RISK ANALYSIS.....</b>	<b>6</b>
3.1	RISK IDENTIFICATION (DEFAULT MODELLING) .....	6
3.2	UPDATING IMPACTS AND CONSEQUENCES .....	7
3.3	RISK ASSESSMENT .....	8
3.4	RISK TREATMENT.....	9
3.5	RISK TREATMENT PLAN MANAGEMENT .....	10

# 1 Introduction

## 1.1 Purpose of the document

The purpose of this document is to help get started quickly with MONARC. It explains the main features of the tool and the necessary steps to deal with a risk with the default settings.

## 1.2 Other documents

“MONARC\_Tool-Doc”: Complete documentation of the tool.

“MONARC\_Method-Doc”: Complete documentation of the method.

## 1.3 Compatibility warning

MONARC application is optimized for “Chrome”. For the moment, please do not use “Internet Explorer”.

## 1.4 Syntax used in the document

 : All numbers in white on a red background are used on print-screen views to provide additional explanations. Explanations are always after the view with the corresponding numbering: “1)” ...

*Italic*: All sentences in italics are some advice.

## 1.5 Syntax used in MONARC

 : Button that always brings up the menu.

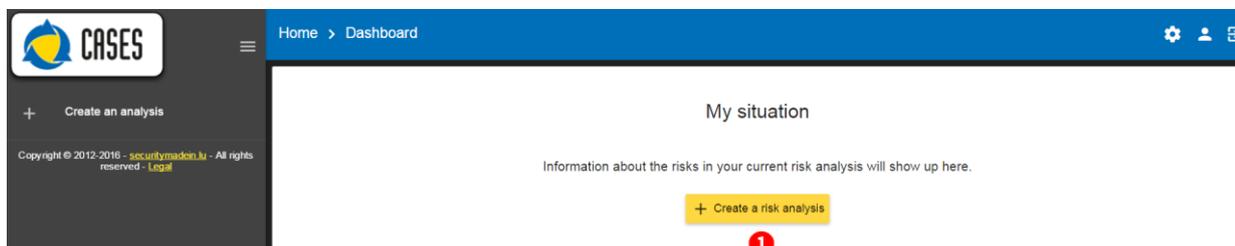
 : Creating/adding something in context (assets, recommendations, etc.).

 : Most fields of MONARC display additional information when the pointer stay unmoved some time.

## 2 Home page

### 2.1 First Connection Screen

At the first connection, the following screen appears:



- 1) Click on “Create a risk analysis”

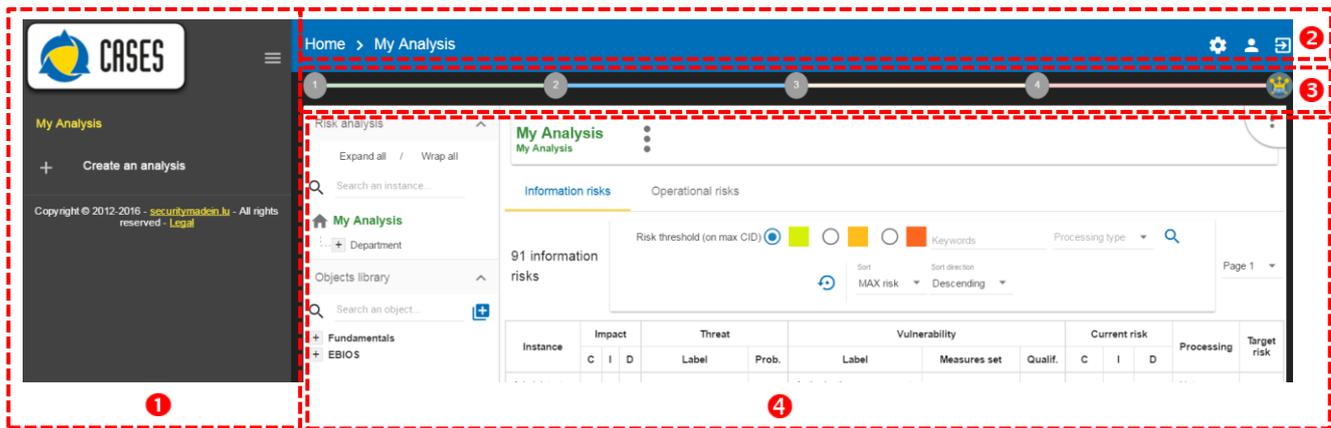
### 2.2 Creating the first risk analysis

After clicking on “Create a risk analysis”, the following pop-up appears:

The screenshot shows a 'Create a new risk analysis' pop-up form. It has a blue header with the title and a close button. The form is divided into two sections: 'Source' and 'Description'. In the 'Source' section, there are two radio buttons: 'CASES model' (selected, marked with a red circle '1') and 'Existing analysis'. Below this is a dropdown menu for 'Modelling CASES' (marked with a red circle '2'). A checkbox for 'Show raw ROLF risks' is present (marked with a red circle '3'). The 'Description' section has a 'Language \*' dropdown (marked with a red circle '4'), a 'Name \*' text field (marked with a red circle '5'), and a 'Description' text field (marked with a red circle '6'). At the bottom are 'Cancel' and 'Create' buttons (marked with a red circle '7').

- 1) Select “CASES model”
- 2) There are at least two choices. Select “Modeling CASES”, this is the default template. It provides sufficient knowledge bases to start an analysis.
- 3) Displays the “raw operational risks table”. This option does not matter right now.
- 4) Select your preferred language for this new analysis.
- 5) Give your analysis a name, for example “My analysis”.
- 6) Optional field, which allows you to describe your analysis with more details.
- 7) If all required fields are filled in, click on “Create”

### 2.3 Description of the main view



1. Analysis list: Create, edit, delete and select analyzes. *Once the analysis is selected, the dashboard can be retracted to optimize the horizontal space by clicking on the symbol ☰.*
2. Navigation pane and management of the customer environment, user rights and information..
3. Access the steps of the method by clicking on numbers 1 to 4.
4. Contextual working areas of analysis.

### 3 Simplified risk analysis

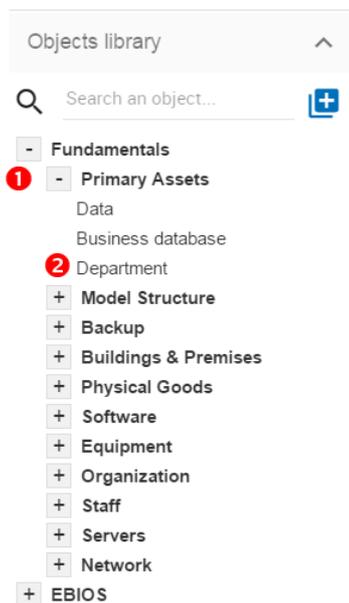
#### 3.1 Risk identification (default modeling)

It is necessary to use the assets of the library and place them in the analysis.

If the risk analysis does not contain any assets, follow the instructions below, otherwise go to the next chapter.

MONARC proposes by default a structure where primary assets (Business) must be placed on the root of the analysis and supporting assets below. In order to simplify this step, two groups of assets have been created:

- 1) **Front-Office:** This asset group provides the identification of the common risks found on the user’s side for a “Human Resources” department (for example, risks related to the office, computers, applications, physical & environmental risks...).
- 2) **Back-Office:** These assets group provide the identification of transversal risks of the organization related to the IT and to organizations in general.



Click on the “+” or the “-” to expand or wrap all categories of the library.

1. In the category “Primary assets” find the asset “Department”
  - a. Click on “Department” and then, by holding down the left mouse button, move the asset to the analysis area just above (Drag and Drop).
2. In the category “Model Structure” find the assets “Front Office” and “Back Office”
  - a. Click on “Front Office” and then, by holding down the left mouse button, move the asset on the asset “Department”, which is now in the analysis area.
  - b. Click on “Back Office” and then, by holding down the left mouse button, move the asset on the asset “Department”, which is now in the analysis area.

Instance	Impact			Threat		Vulnerability			Current risk			Processing	Target risk
	C	I	D	Label	Prob.	Label	Measures set	Qualif.	C	I	D		
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not processed	-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not processed	-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not processed	-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-	-	-	Not processed	-
Administrator workstations	-	-	-		-	Programs can be		-	-	-	-	Not processed	-

- 1) The risk analysis now offers a model for “Department”.
- 2) The “Front Office” now offers a default identification of the risks on the users’ side.
- 3) The “Back Office” now offers a default identification of the risks, for IT and organization.
- 4) The total number of risks in this model is 91 (in this case).

Note: Identified risks by default are the risks commonly encountered and supposed to be significant, they do not claim to be exhaustive.

### 3.2 Updating impacts and consequences

The aim is to define impacts and consequences for primary assets that can result from an occurrence of a risk from the model.

In the case of this analysis, the primary asset is “Department”.

The screenshot shows the MONARC interface. On the left is a sidebar with a tree view under 'My Analysis' containing 'Department' (marked with a red 1) and its sub-items: Front Office, Service office, Printer, Physical documents, Employees, User workstations, Specific software, Back Office, Building, IT room, System administrator, Administrator workstations, Server management, Backup management, and Network and Telecom. The main panel displays the 'Department' asset (marked with a red 2) with a context menu (marked with a red 3) open, showing options: Edit impacts, See object in the library, Detach, Import analysis, and Export instance. Below the asset details is a table of 91 information risks.

Instance	Impact			Threat		Vulnerability			Current risk			Processing	Target risk
	C	I	D	Label	Prob.	Label	Measures set	Qualif.	C	I	D		
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not processed	-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not processed	-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not processed	-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-	-	-	Not processed	-

- 1) Click on the primary asset “Department”.
- 2) Click on the symbol to display the context menu of the asset.
- 3) Click on “Edit impacts”.

The pop-up below appears:

The screenshot shows a dialog box titled 'Update instance "Department" details'. It features a 'Consequences' section with a table of impact values. A 'Max' column on the right indicates the maximum value for each category. The 'Save' button is highlighted in orange.

Category	Reputation	Operational	Legal	Financial	Personal	Max
Confidentiality	2	0	2	Unknown	3	3
Integrity	2	0	1	Unknown	2	2
Availability	2	0	2	Unknown	2	2

- 1) Consultation of impact scales is done through the menu at the top right of the screen.

*By leaving the pointer unmoved over the numbers, the meaning of this number appears after one second.*

When one of the criteria C (confidentiality), I (integrity) or A (availability) is allocated, there is a need to ask : what are the consequences on the company, and more particularly on its ROLFP, i.e. its “Reputation”, its “Operation”, its “Legal”, its “Finances” or the impact on the “Person” (in the sense of personal data).

In the case of the above figure, the “3” (out of 5) impact on confidentiality, is explained by the maximum value ROLFP regarding confidentiality. Example, “3” is the consequence for the person in case of disclosure of his personal file.

### 3.3 Risk assessment

Instance	Impact			Threat		Vulnerability			Current risk			Processing	Target risk
	C	I	D	Label	Prob.	Label	Measures set	Qualif.	C	I	D		
Building	3	2	2	Theft or destruction of media, documents or equipment	-	The principle of least privilege is not applied		-	-	-	-	Not processed	-
Building	3	2	2	Theft or destruction of media, documents or equipment	-	Authorisation management is flawed		-	-	-	-	Not processed	-

- 1) Click on a secondary asset, for example “Building”.
- 2) CIA criteria that have been assigned to the “Department” are inherited by default and are no longer required.
- 3) The threat: “Theft or destruction of media, documents or equipment” is a physical threat that expresses fear of being robbed or destroyed materials.
- 4) This is an estimate of the probability on a scale of 1 to 4 that the threat occurs. Take, for example, the case of a very large company where this threat is above average, so “3”.
- 5) Vulnerability: “The principle of least privilege is not applied”. The security principles searched are to know who has access rights and whether they related to the duties of the people involved.
- 6) Controls in place: Describe, in a factual manner, the security controls in place regarding this vulnerability or, more broadly, the risk in question. Take, for example, a second unfavorable case, for example a hospital where the whole building is like a public area.
- 7) In relation to the measure in place (point 6 above), the vulnerability is therefore maximum “5” out of 5.

*By leaving the pointer on most fields, a tooltip appears after 1 second.*

All the parameters for calculating the risk are present, the current risk is therefore calculated based on the CIA values, which are directly dependent on the threat.

Risk analysis

Expand all / Wrap all

Search an instance...

My Analysis

- Department
  - Front Office
    - Service office
    - Printer
    - Physical documents
  - Employees
  - User workstations
  - Specific software
  - Back Office
    - Building

Confidentiality: 3 (inherited) Integrity: 2 (inherited) Availability: 2 (inherited)

5 information risks

Risk threshold (on max CID) [Color indicators] Keywords [Search icon] [Refresh icon] Sort: MAX risk [Dropdown]

Sort direction: Descending [Dropdown]

Instance	Impact			Threat		Vulnerability			Current risk			Processing	Target risk
	C	I	D	Label	Prob.	Label	Measures set	Qualif.	C	I	D		
Building	3	2	2	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	The building is accessible by all visitors without any access control	5	45		30	Not processed <span style="color:red">1</span>	45

1) Click “Not processed” in order to call the Risk Processing view.

### 3.4 Risk treatment

The risk treatment consists in proposing one of the 4 types of treatment, knowing that most of the time the treatment is to reduce the risk by allocating a control, or to accept a weak risk.

Risk analysis

Expand all / Wrap all

Search an instance...

My Analysis

- Department
  - Front Office
    - Service office
    - Printer
    - Physical documents
  - Employees
  - User workstations
  - Specific software
  - Back Office
    - Building
    - IT room
    - System administrator
    - Administrator workstations
    - Server management
    - Backup management
    - Network and Telecom
    - IT organization
    - Software development

Confidentiality: 3 (inherited) Integrity: 2 (inherited) Availability: 2 (inherited)

← Back to the list

Risk sheet

	C	I	D
Current risk	45		30
Target risk	45		30

Instance: Department > Back Office > Building

Threat: Theft or destruction of media, documents or equipment

Threat probability: 3 - Could happen occasionally

Vulnerability: The principle of least privilege is not applied

Vulnerability qualification: 5 - Very strong vulnerability. No measures have been implemented. Very low maturity or no maturity at all.

Measures set: The building is accessible by all visitors without any access control

Recommendations 1

Search a recomme... +

Processing type: Not processed 2

Reduce vulnerability by: 0 3

Security referential: 11.1.2 - Physical entry controls

Save

- 1) Create a recommendation.
- 2) Define the treatment type (according to ISO / IEC 27005).
- 3) Estimate the risk-reducing value in order to define the residual risk.

**Risk analysis**

Expand all / Wrap all

Search instance...

**My Analysis**

- Department
  - Front Office
    - Service office
    - Printer
    - Physical documents
    - Employees
    - User workstations
  - Specific software
  - Back Office
    - Building**
    - IT room
    - System administrator
    - Administrator workstations
    - Server management
    - Backup management
    - Network and Telecom
    - IT organization
    - Software development

**Objects library**

Search an object...

- Fundamentals
  - Primary Assets

**Building**

Confidentiality: 3 (inherited) Integrity: 2 (inherited) Availability: 2 (inherited)

← Back to the list

**Risk sheet**

	C	I	D
Current risk	45		30
Target risk	18		12

Instance: Department > Back Office > Building

**Threat**: Theft or destruction of media, documents or equipment

**Threat probability**: 3 - Could happen occasionally

**Vulnerability**: The principle of least privilege is not applied

**Vulnerability qualification**: 5 - Very strong vulnerability: No measures have been implemented. Very low maturity or no maturity at all.

**Measures set**: The building is accessible by all visitors without any access control

**Recommendations**: Entry \*\*\* > Move the reception to the entrance of the building to control the access of each incoming person

Search a recomme... +

**Processing type**: Reduction

**Reduce vulnerability by**: 3

**Security referential**: 11.1.2 - Physical entry controls

1 Save

1) Once the recommendation is created and the risk card validated, the risk is treated.

### 3.5 Risk treatment plan management

In that case, the risk treatment plan only consists in one risk, but once all risks are treated, all risks and information risk recommendations will be in the treatment plan.

1 2 3 4

**Risks evaluation and treatment**

- Risks estimation, evaluation and processing
- Risk treatment plan management 1

Deliverable: final report

1) The call of the pop-up is done by clicking on the 3rd step of the method and “Risk treatment plan management”.

**Risk treatment plan management**

Reset positions

	Recommendation	Imp.	Asset	Measures set	Current risk	Target risk
↓	Entry Move the reception to the entrance of the building to control the access of each incoming person	***	Building	The building is accessible by all visitors without any access control	45	18

A final report of risk analysis can be generated by clicking on the 3rd step of the method and “Deliverable: final report”.

Note: Deliverables are only relevant when the MONARC method has been fully processed and all information has been entered.