Quick Start

NC3 Luxembourg

Version 2024-11-25

Table of Contents

Chapter 1. Introduction

1.1. Purpose

The purpose of this document is to help you get started quickly with MONARC. The Quick Start Guide outlines the tool's main features and shows the essential steps for addressing risks using the default settings.

1.2. Other documents

ⓘ

- **User Guide**: Provides the complete documentation of the tool.
- **Method Guide**: Provides the complete documentation of the method.
- **Technical Guide**: Provides the complete technical documentation of the tool.

1.3. Syntax used in the document

1 All numbers displayed in white on an orange background are used in print-screen views to provide additional explanations. Explanations are always after the view with the corresponding numbering. **i.e.** 1.

`Reference` MONARC Reference

1.4. Syntax used in MONARC

⋮ The three-dot menu icon brings brings up the menu items.

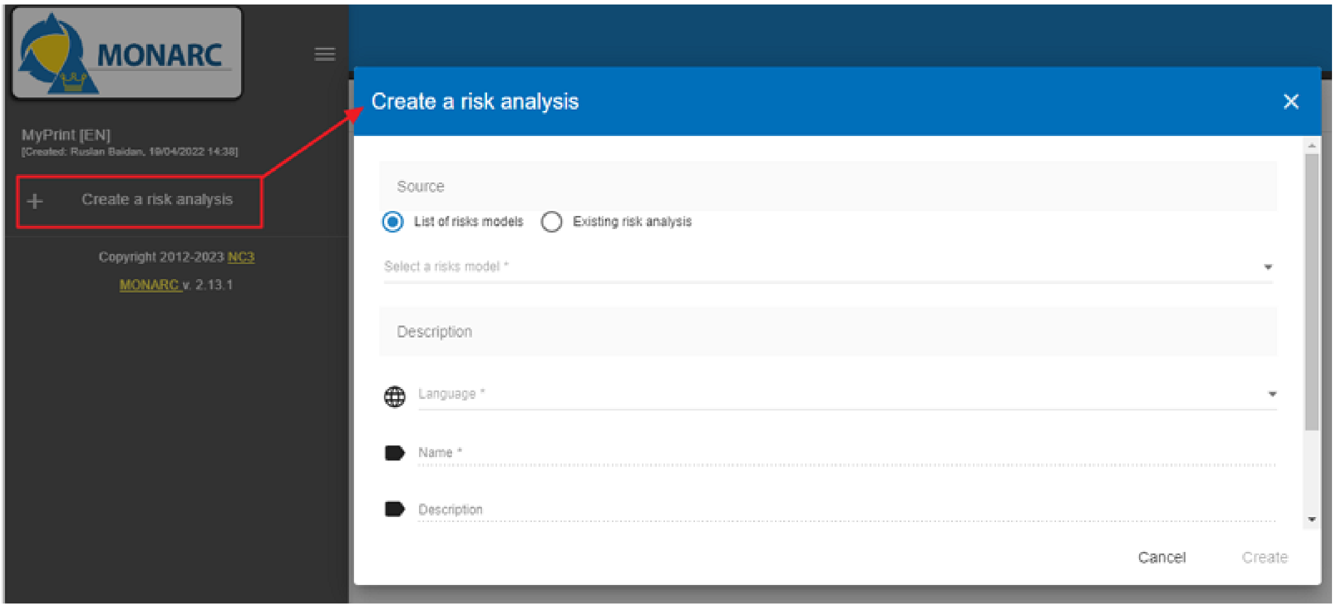
⊞ Create/add something in context (assets, recommendations, etc.).

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

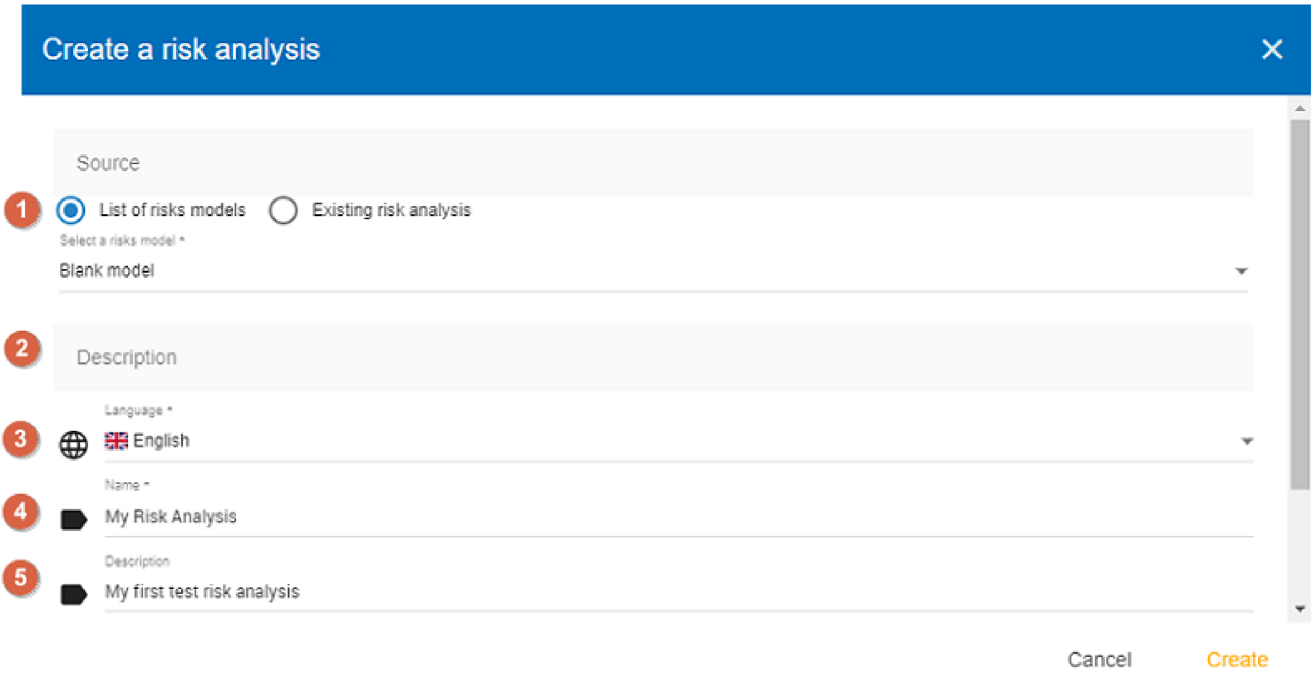
⬇ Export any table (.csv) or graphic (.png).

Chapter 2. Creating the first risk analysis

After clicking on `Create a risk analysis`,



the following pop-up appears:



● List of risks models ○ Existing risk analysis

Select a risks model *: Blank model

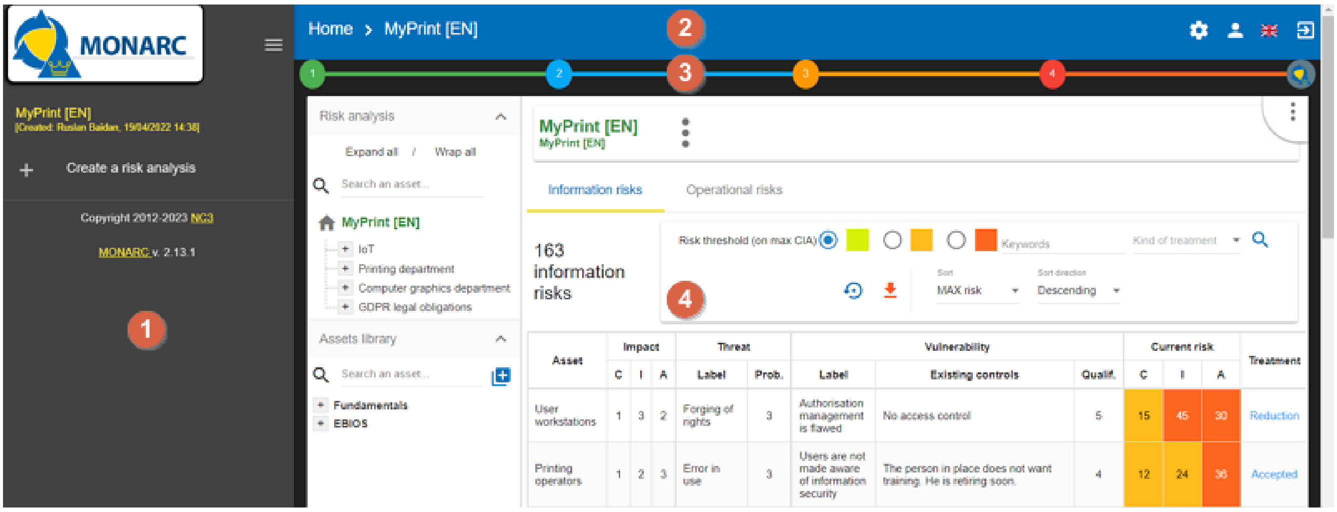
Language *: English

Name *: My Risk Analysis

Description: My first test risk analysis

1. Select `List of risks models`
2. There are at least two choices. Select `Modelling NC3`. Modelling NC3 is the default template made available by the MONARC editor. It provides sufficient knowledge bases to start a risk analysis. This option should be used by default to start a new risk analysis.
3. Select your preferred language for this new analysis. (FR/EN/DE/NL)
4. Give a name for your risk analysis, for example, *My analysis*.
5. Optional field, which allows you to describe your analysis in more detail.

Chapter 3. Description of the main view



Asset	Impact			Threat		Vulnerability			Current risk			Treatment
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A	
User workstations	1	3	2	Forging of rights	3	Authorisation management is flawed	No access control	5	15	45	30	Reduction
Printing operators	1	2	3	Error in use	3	Users are not made aware of information security	The person in place does not want training. He is retiring soon.	4	12	24	36	Accepted

1. Risk Analyses panel: Create and select a risk analysis. Once the analysis is selected, the left column can be retracted to optimize the horizontal space by clicking on the icon ☰.
2. Navigation panel: User administration and account management.
3. Access to steps of the method by clicking on numbers 1 to 4.
4. Contextual working areas of analysis.

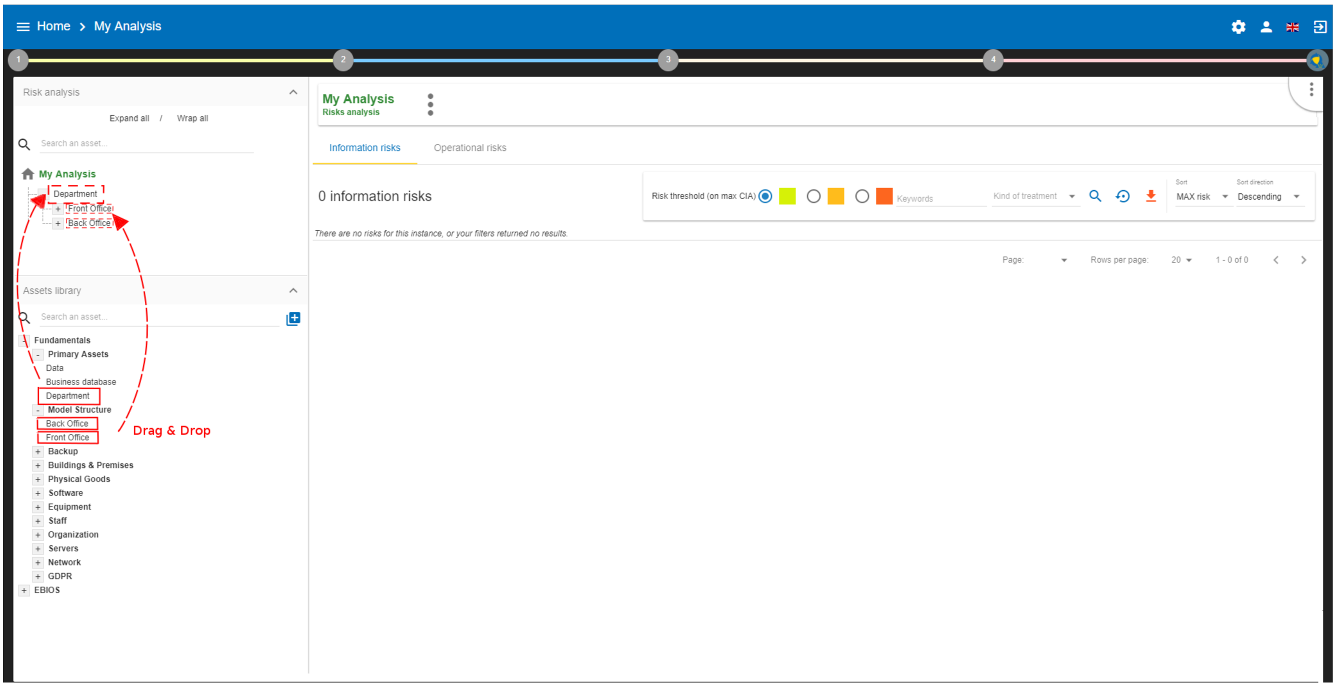
Chapter 4. Simplified risk analysis

4.1. Risk identification (default modelling)

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.

By default, MONARC suggests a structure where primary assets (business assets) are placed at the root of the analysis, with supporting assets organized beneath them. In order to simplify this step, two groups of assets have been created:

- `Front-Office`: This asset group identifies common risks associated with a 'Human Resources' department from the user's perspective, including risks related to office spaces, computers, applications, and physical and environmental factors.
- `Back-Office`: This asset group identifies cross-functional risks within the organization, specifically those related to IT and general organizational functions.



0 information risks

Risk threshold (on max CIA) ● 🟩 ○ 🟨 ○ 🟧

Sort: MAX risk

Sort direction: Descending

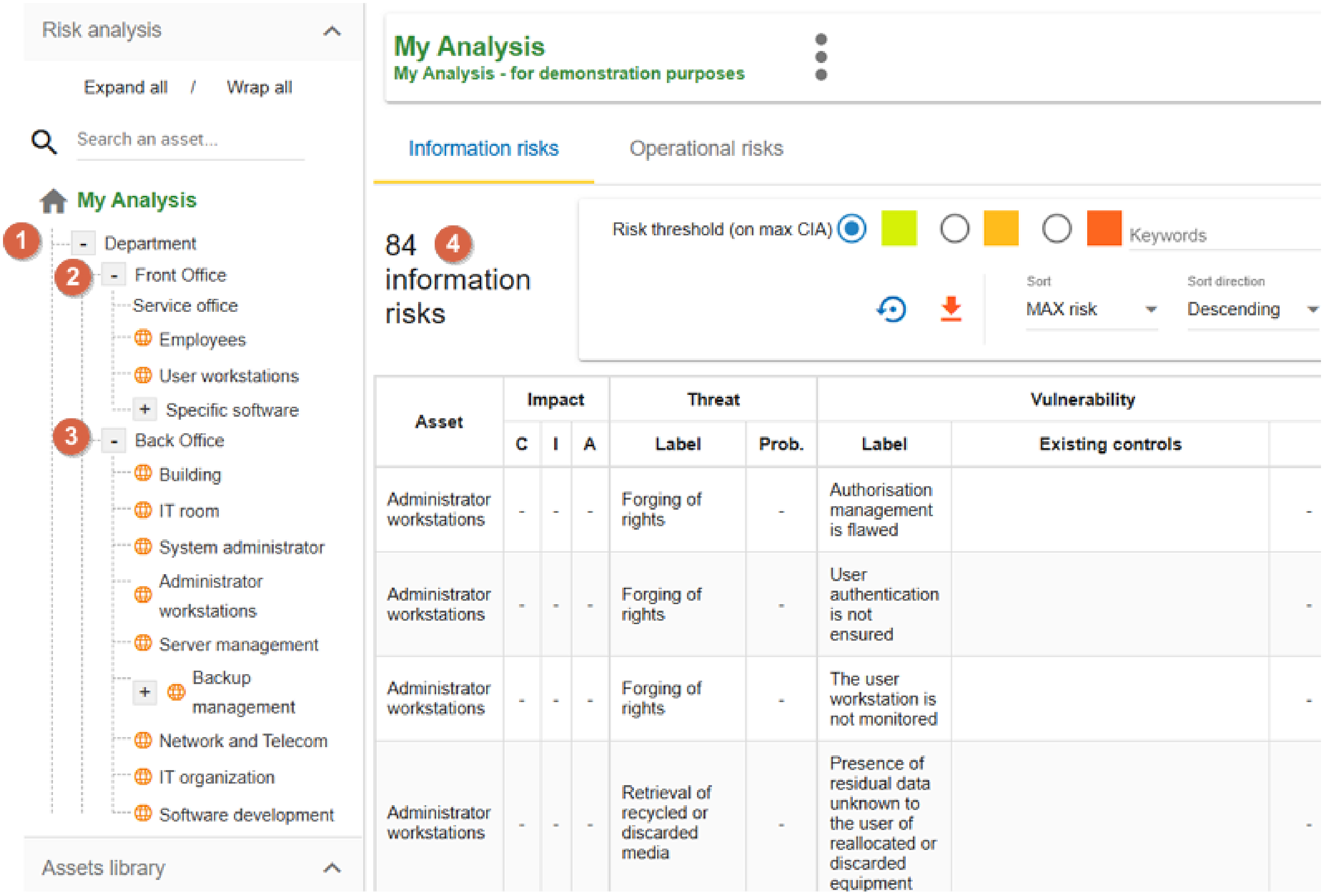
There are no risks for this instance, or your filters returned no results.

Rows per page: 20

1 - 0 of 0

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

1. In the category `Primary assets`, 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` and then, by holding down the left mouse button, move the asset to the asset Department, which is now in the analysis area.



84 information risks

Risk threshold (on max CIA) ● 🟩 ○ 🟧 ○ 🟥

Sort: MAX risk

Sort direction: Descending

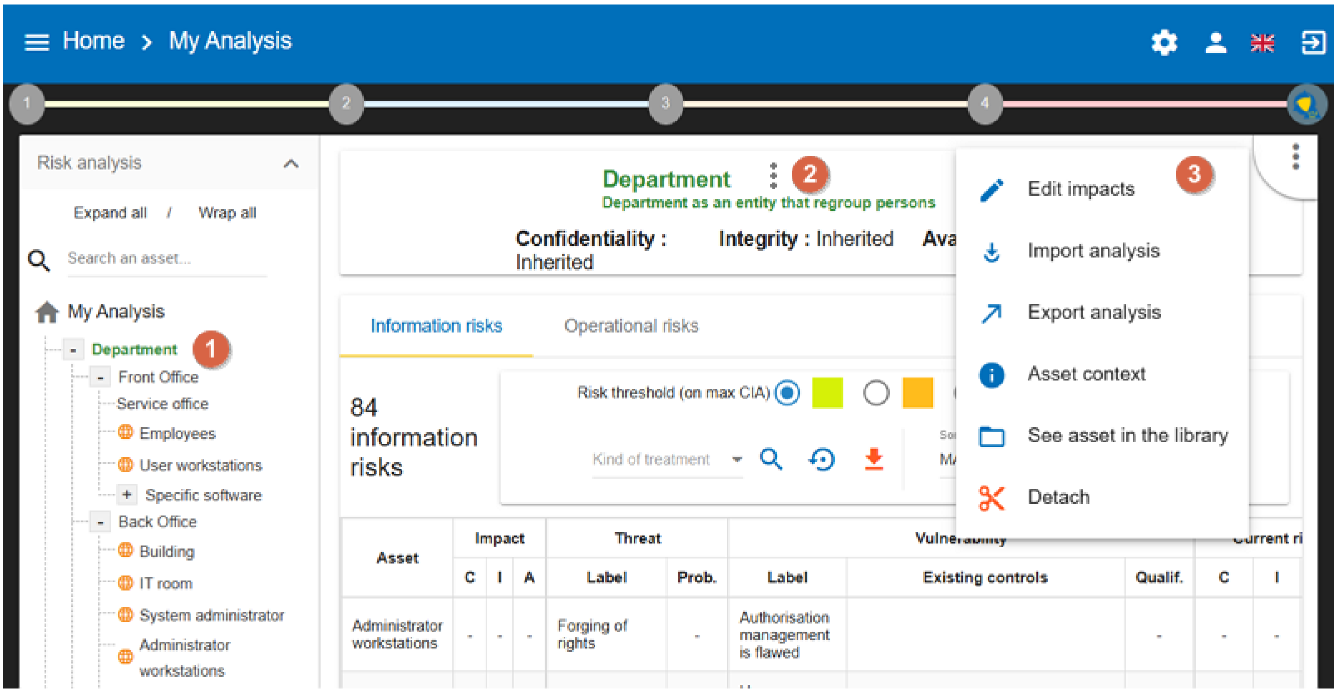
Asset	Impact			Threat		Vulnerability		
	C	I	A	Label	Prob.	Label	Existing controls	
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed		-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured		-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored		-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-

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 84 (in this case).

> ❗ The Identified risks are those commonly encountered and considered significant by default, though they are not intended to be exhaustive.

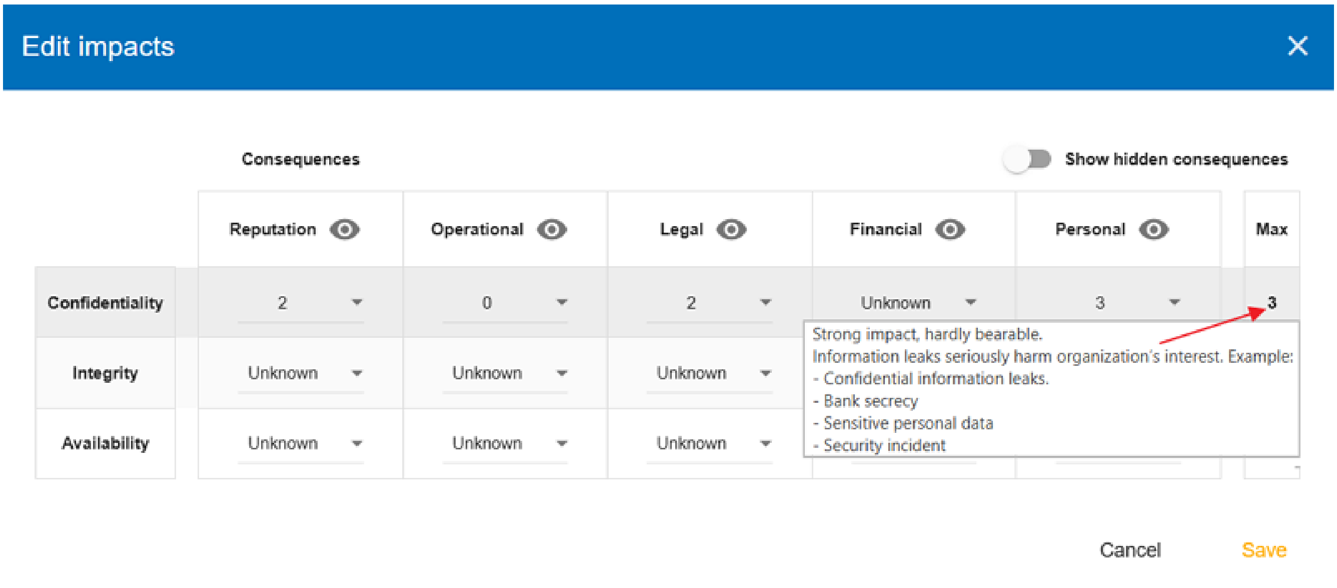
4.2. Edit impacts and consequences

The goal is to define the impacts and consequences on primary assets that may result from a risk occurring within the model. In this analysis, the primary asset is the *Department*.



1. Click on the primary asset `Department`.
2. Click on the icon ⋮ to display the context menu of the asset.
3. Click on `Edit impacts`.

The pop-up below appears.


Edit impacts ✕

Consequences — Show hidden consequences

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

Strong impact, hardly bearable.
Information leaks seriously harm organization's interest. Example:
- Confidential information leaks.
- Bank secrecy
- Sensitive personal data
- Security incident

Cancel Save

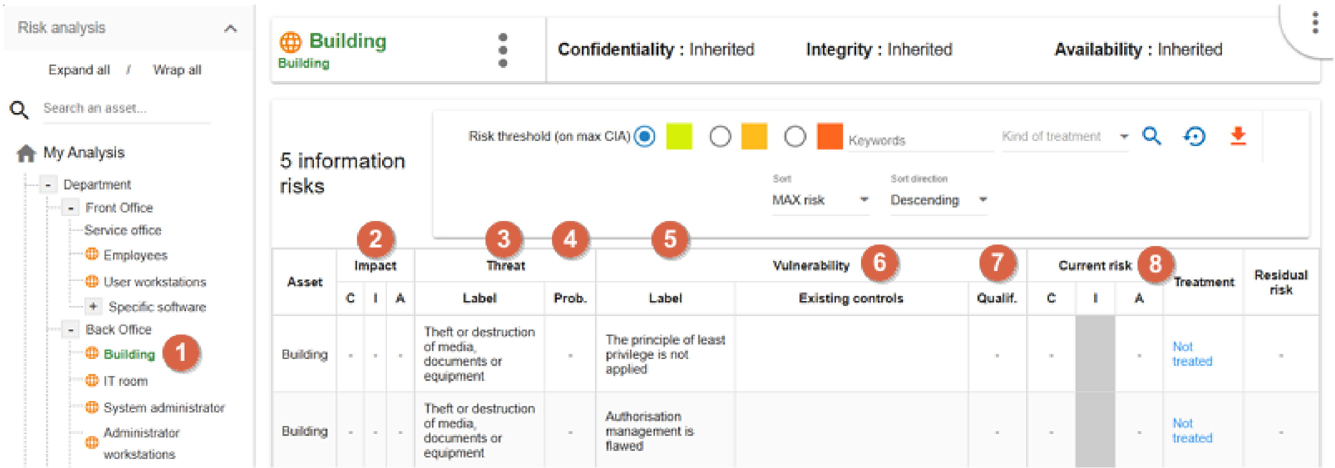
1. Consultation of impact scales is done through the menu at the top right of the screen.

> *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 **R**eputation, its **O**peration, its **L**egal, its **F**inances or the impact on the **P**erson (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.

4.3. Risk assessment



Building
Building

Confidentiality : Inherited Integrity : Inherited Availability : Inherited

5 information risks

Risk threshold (on max CIA) ● 🟨 ○ 🟧 ○ 🟥 Keywords Kind of treatment

Sort: MAX risk Sort direction: Descending

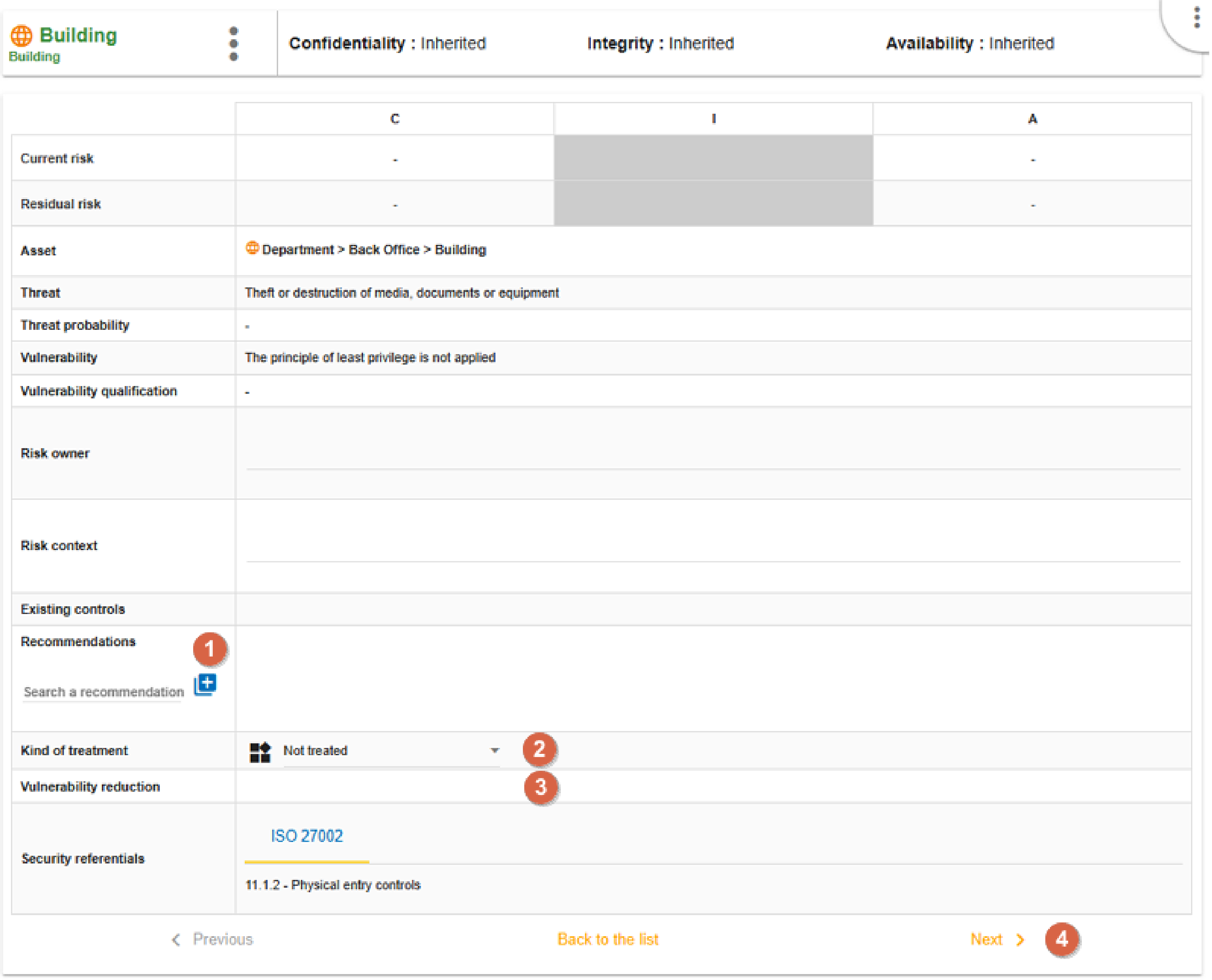
Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Building	-	-	-	Theft or destruction of media, documents or equipment	-	The principle of least privilege is not applied		-	-		-	Not treated	-
Building	-	-	-	Theft or destruction of media, documents or equipment	-	Authorisation management is flawed		-	-		-	Not treated	-

1. Click on a secondary asset, for example `Building`.
2. `CIA Impact`: It has been assigned to the *Department* and is inherited by default, so no further action is required.
3. `Threat`: *Theft or destruction of media, documents or equipment* is a physical threat that expresses fear of being robbed or destroyed materials.
4. `Probability (Prob.)`: 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 focus on determining who has access rights and whether those rights align with the responsibilities of the individuals involved.
6. `Existing controls`: 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 unfavourable case, for example a hospital where the whole building is like a public area.
7. `Qualification (Qualif.)`: Concerning the measure in place (point 6 above), the vulnerability qualification is therefore maximum of **5** out of 5.
8. `Current Risk` : 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.

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

4.4. Risk treatment

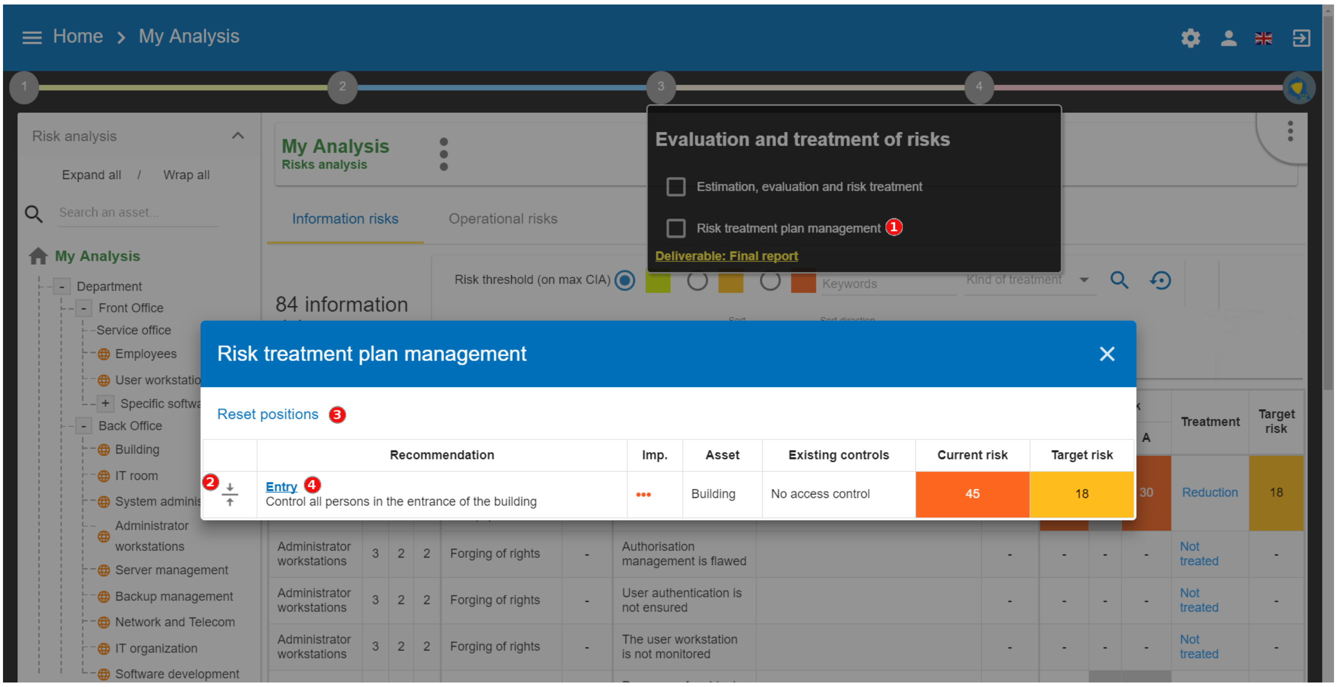
The risk treatment consists of proposing one of the 4 types of treatment, knowing that most of the time the treatment is to reduce the risk by allocating a control, or to accept a weak risk. To access the risk treatment table, click on `Not treated` in the *Treatment column.*



	C	I	A
Current risk	-		-
Residual risk	-		-
Asset	Department > Back Office > Building		
Threat	Theft or destruction of media, documents or equipment		
Threat probability	-		
Vulnerability	The principle of least privilege is not applied		
Vulnerability qualification	-		
Risk owner			
Risk context			
Existing controls			
Recommendations Search a recommendation			
Kind of treatment	Not treated		
Vulnerability reduction			
Security referentials	ISO 27002 11.1.2 - Physical entry controls		

1. Create one or many recommendations.
2. Define the treatment type (according to ISO / IEC 27005).
3. Estimate the risk-reducing value in order to define the residual risk.
4. Save the treatment (or click ‘Next’ in case you do more than one risk treatment at once).

4.5. Risk treatment plan management



Evaluation and treatment of risks

□ Estimation, evaluation and risk treatment

□ Risk treatment plan management 1

Deliverable: Final report

Risk treatment plan management

Reset positions 3

	Recommendation	Imp.	Asset	Existing controls	Current risk	Target risk
2	Entry 4 Control all persons in the entrance of the building	•••	Building	No access control	45	18

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

1. The call of the pop-up is done by clicking on the 3rd step of the method (Evaluation and treatment of risks) and choosing the link `Risk treatment plan management`.
2. You can order the recommendation positions by holding down the left mouse button on the icon ↕ and moving it.
3. Reset the positions in importance order (Imp.)
4. Edit recommendation

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

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