OPTIMISED RISK ANALYSIS

www.monarc.lu

Quick Start

CASES Luxembourg

Table of Contents

1. Introduction

1.1. Purpose

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

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

1.3. 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. **i.e.** 1.

`Reference`

MONARC Reference

1.4. Syntax used in MONARC

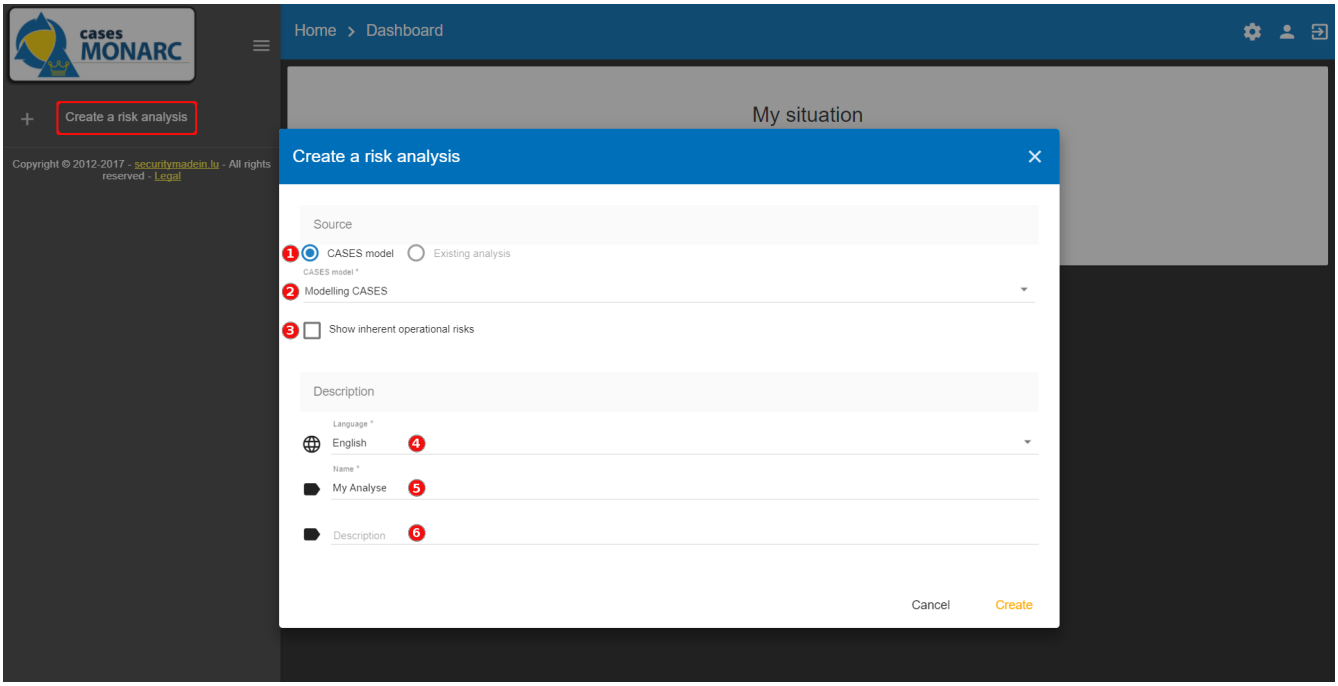
Button that always brings up the menu.

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

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

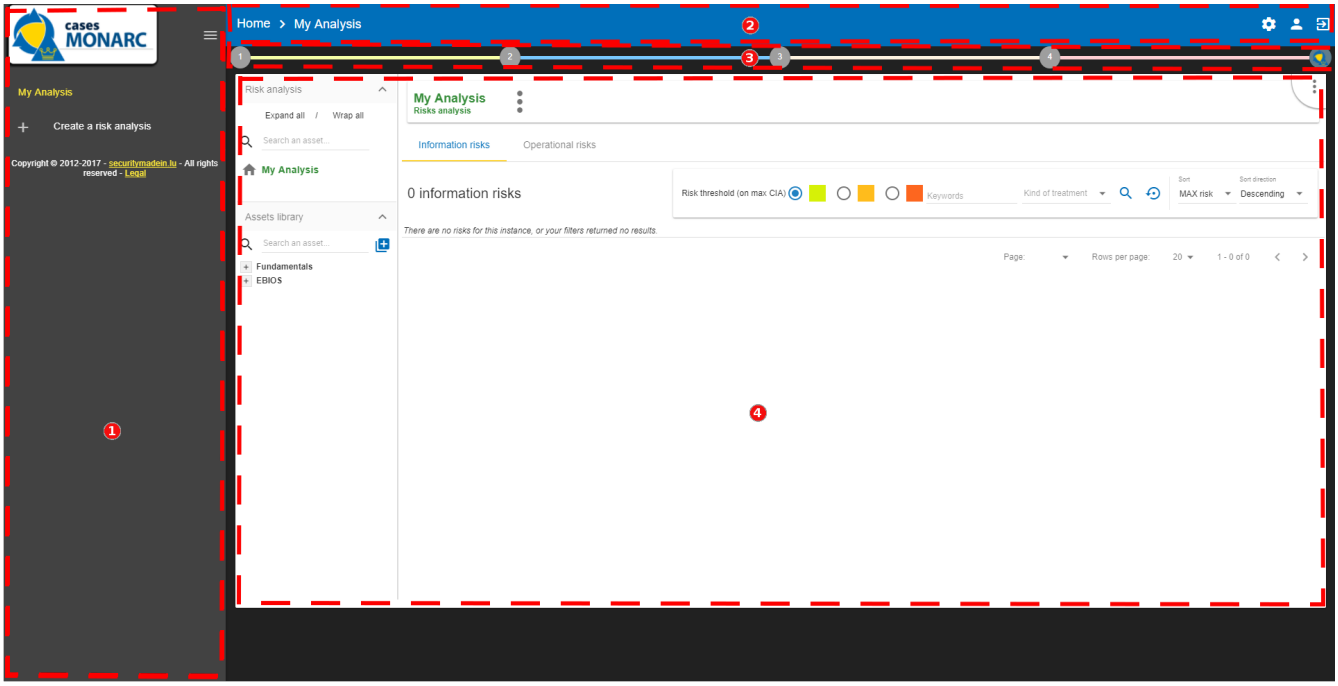
2. Creating the first risk analysis

After clicking on `Create a risk analysis`, the following pop-up appear



1. Select `CASES model`
2. There are at least two choices. Select `Modelling CASES`, this is the default template. It provides sufficient knowledge bases to start an analysis.
3. `Show inherent operational risks`. This option does not matter right now.
4. Select your preferred language for this new analysis. (FR/EN/DE/NL)
5. Give your analysis a name, for example *My analysis*.
6. Optional field, which allows you to describe your analysis with more details.

3. Description of the main view



1. Risk Analyses panel: Create and select a risk analysis. Once the analysis is selected, the

dashboard can be retracted to optimize the horizontal space by clicking on the symbol .

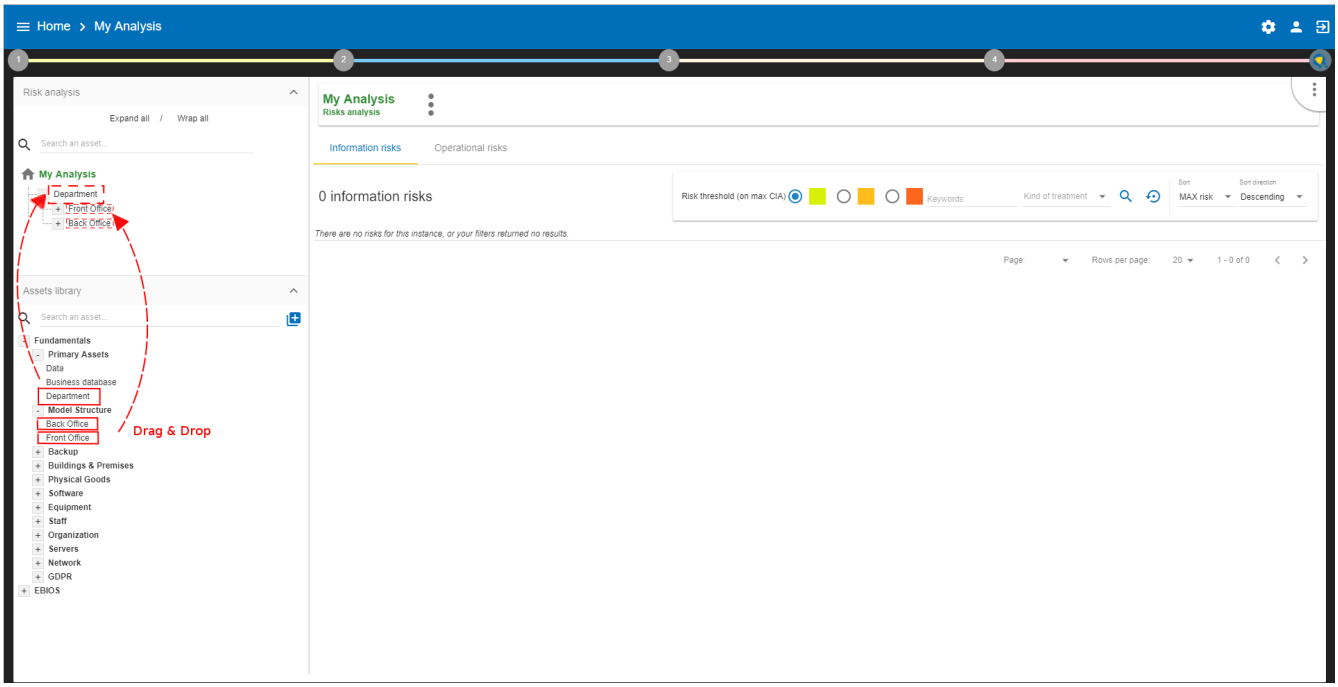
2. Navigation panel, users administration and account management.
3. Access to steps of the method by clicking on numbers 1 to 4.
4. Contextual working areas of analysis.

4. Simplified risk analysis

4.1. Risk identification (default modeling)

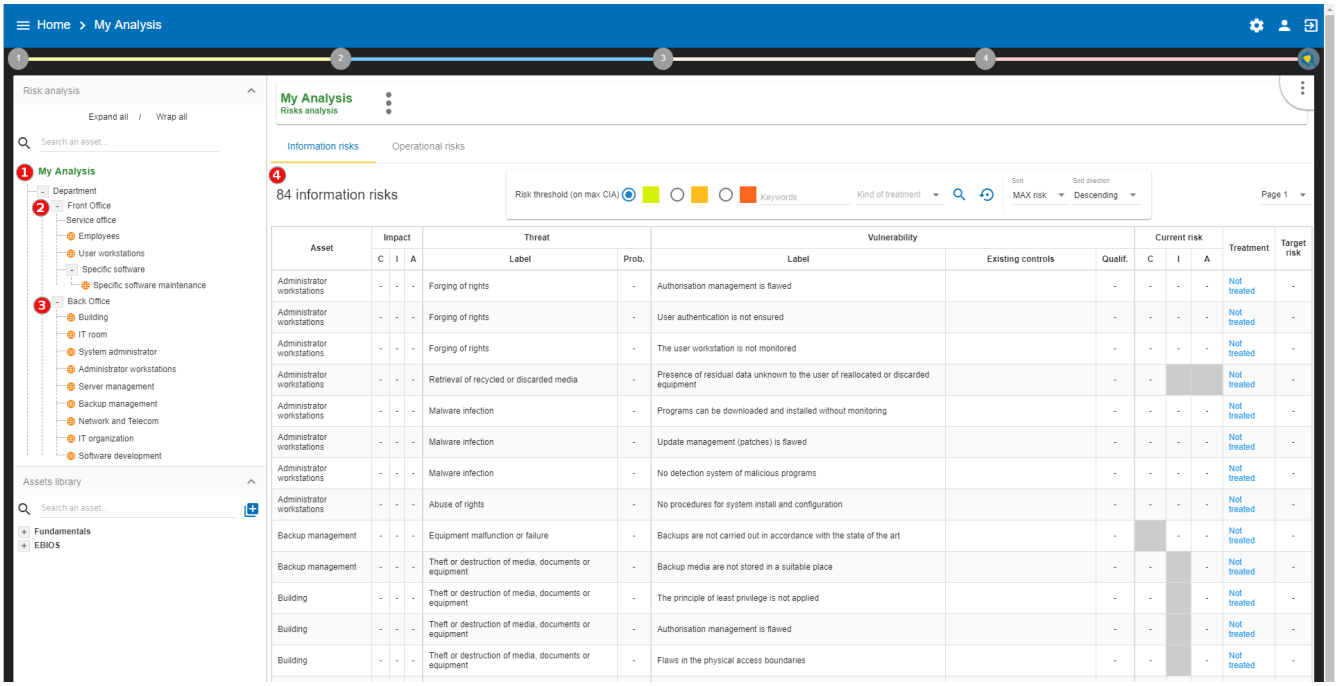
It is necessary to use the assets of the library and place them in the analysis. If the risk analysis does not contain any assets, follow the instructions below, otherwise go to the next chapter. MONARC proposes by default a structure where primary assets (Business) must be placed on the root of the analysis and supporting assets below. In order to simplify this step, two groups of assets have been created:

- `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...).
- `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`, 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 on the asset Department, which is now in the analysis area.

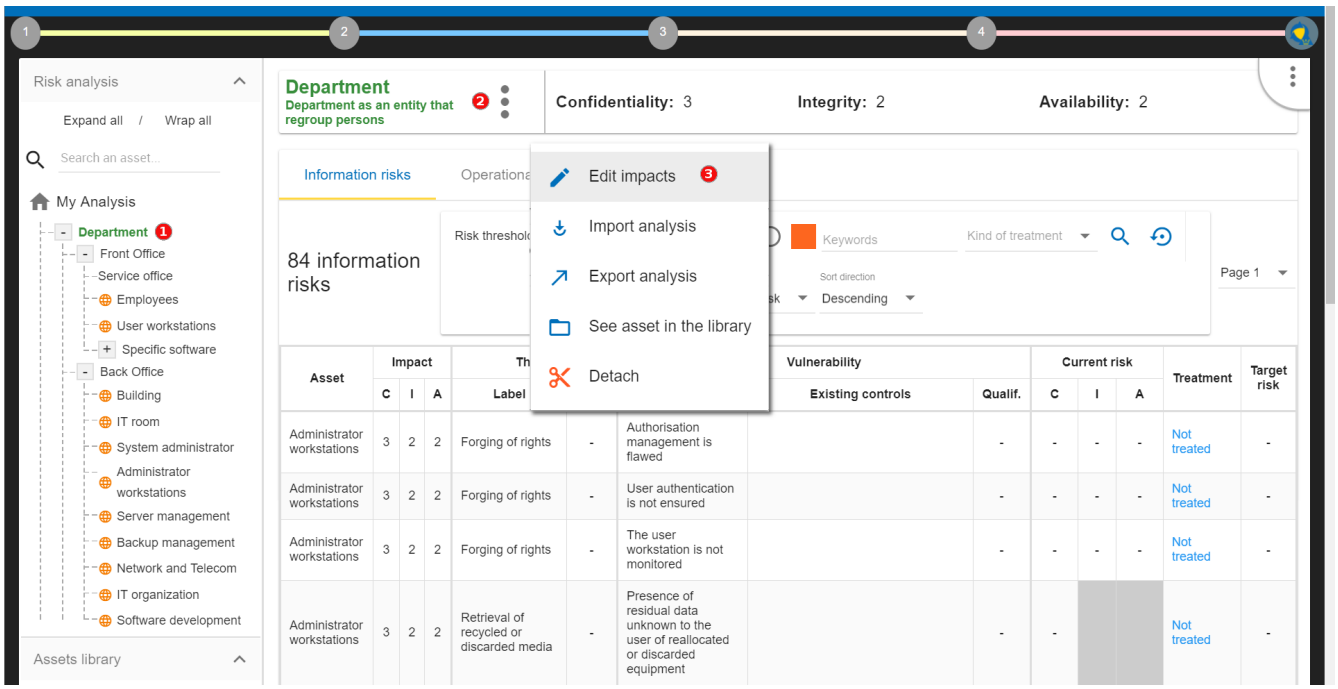


1. The risk analysis now offers a model for *Department*.
2. The *Front Office* now offers a default identification of the risks on the users' side.
3. The *Back Office* now offers a default identification of the risks, for IT and organization.
4. The total number of risks in this model is 84 (in this case).

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

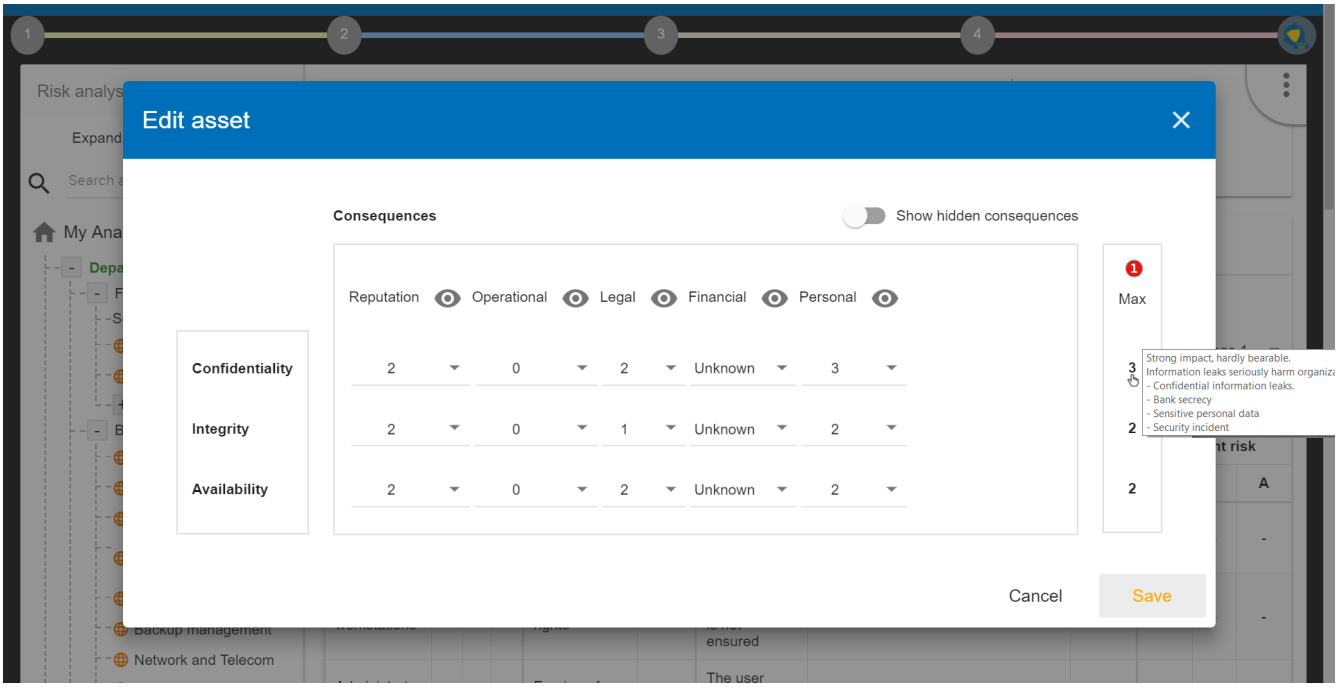
4.2. Edit impacts and consequences

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*.



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.



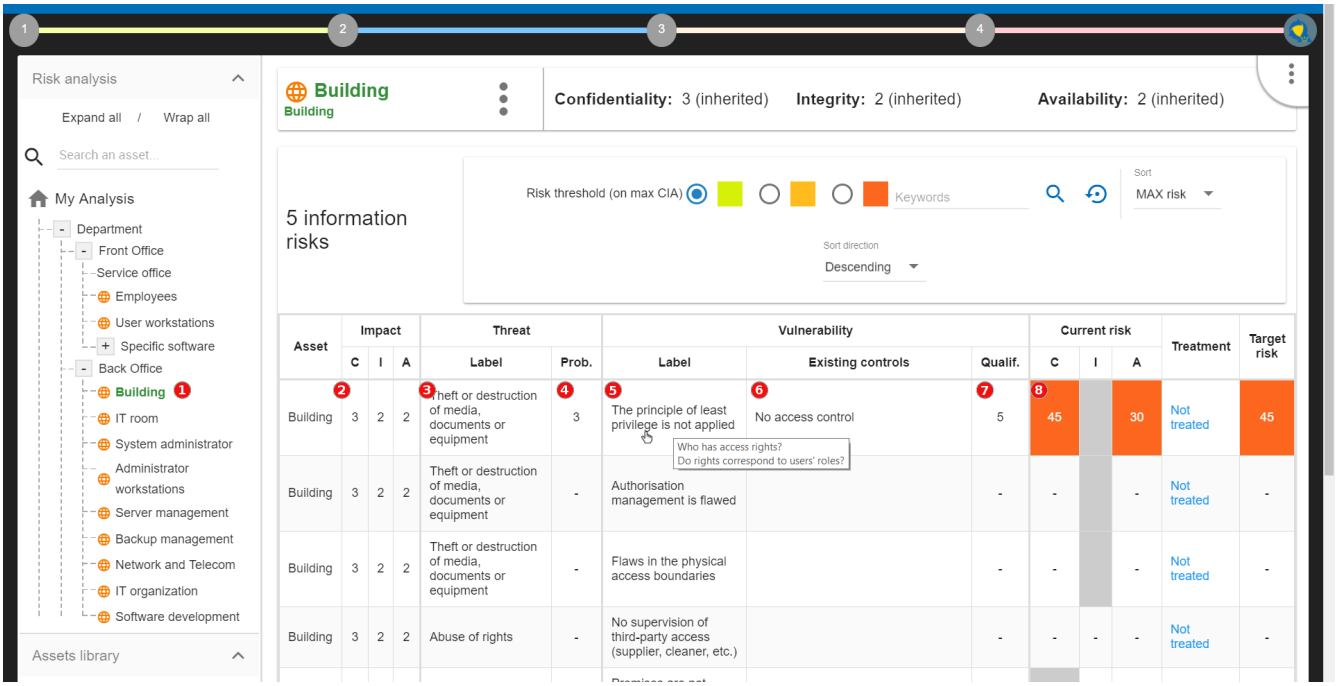
1. Consultation of impact scales is done through the menu at the top right of the screen.

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

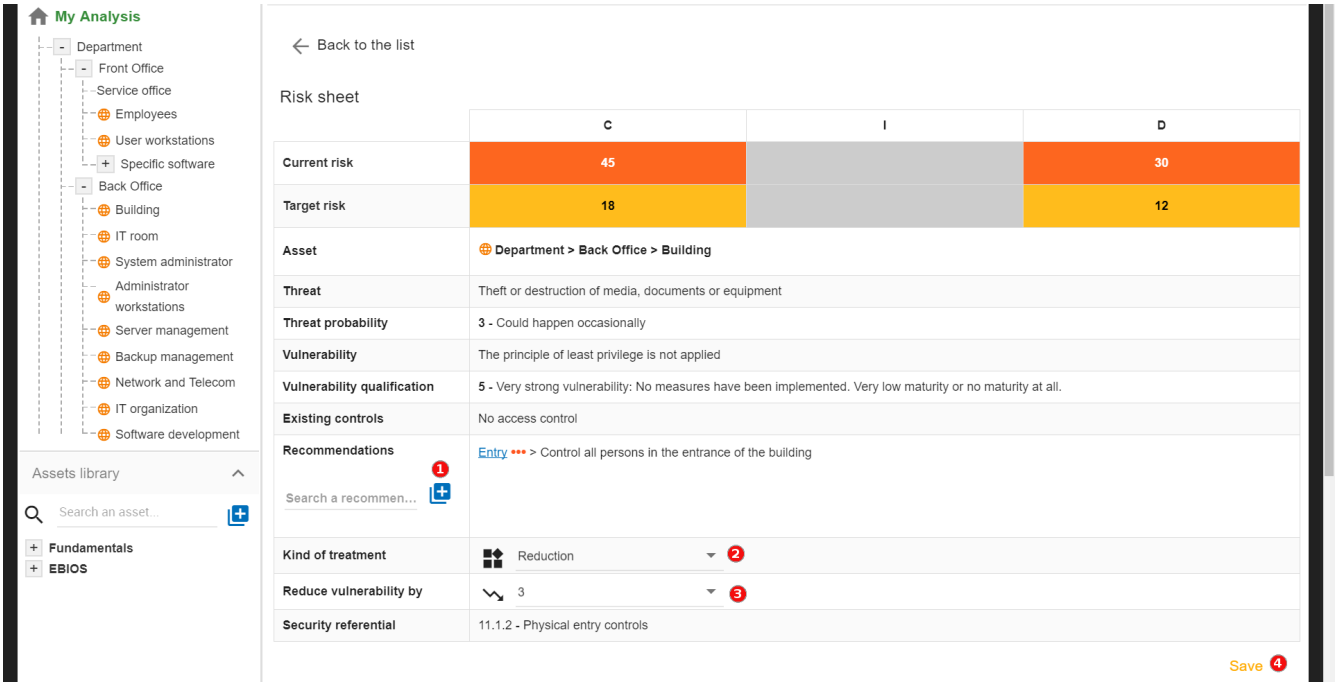


1. Click on a secondary asset, for example `Building`.
2. `CIA Impact`: It has been assigned to the *Department* is inherited by default and are no longer required.
3. `Threat`: *Theft or destruction of media, documents or equipment* is a physical threat that expresses fear of being robbed or destroyed 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 searched are to know who has access rights and whether they related to the duties of the people 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 unfavorable case, for example a hospital where the whole building is like a public area.
7. `Qualification (Qualif.)` : In relation to the measure in place (point 6 above), the vulnerability qualification is therefore maximum **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.

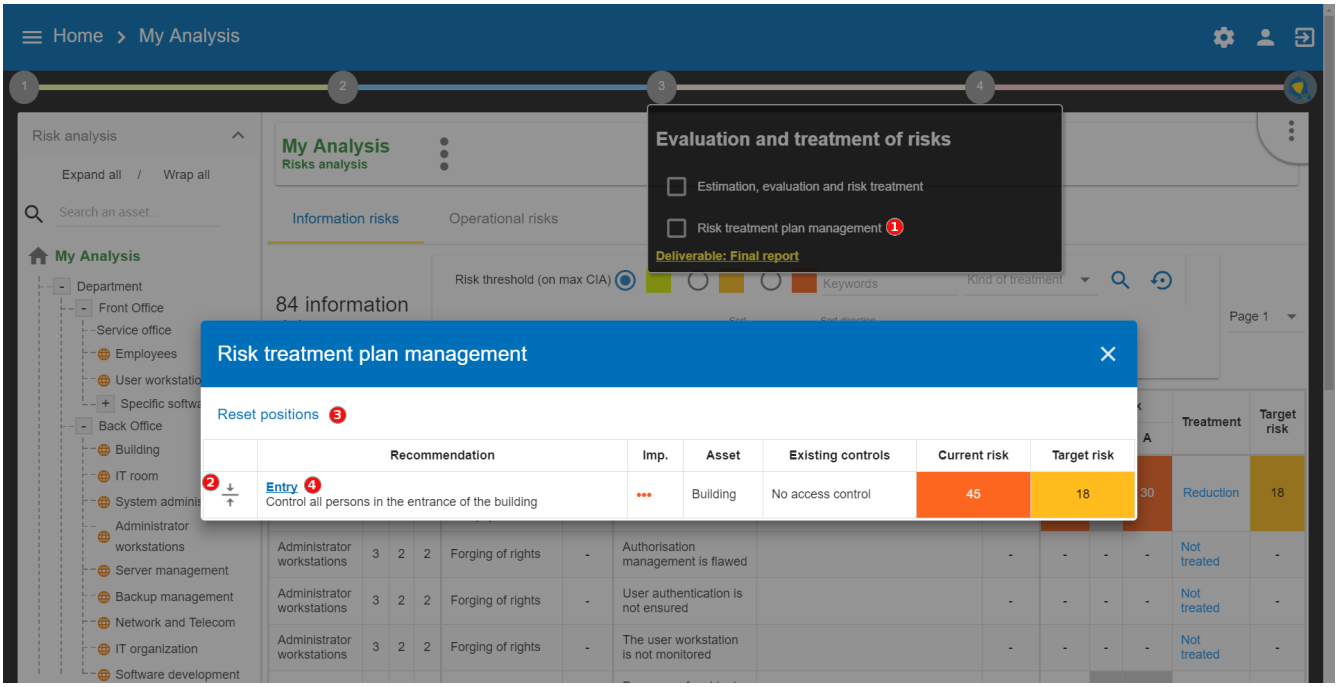
4.4. Risk treatment

The risk treatment consists 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. To access click on `Not treated` in *Treatment column*.



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.

4.5. 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. The call of the pop-up is done by clicking on the 3rd step of the method and `Risk treatment plan management`.

2. Order the recommendation positions holding down the left mouse button on symbol  and move it.
3. Reset the positions in importance order (Imp.)
4. Edit recommendation

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

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