

**MONARC**

**Optimised Risk Analysis Method**

**Documentation of the tool**

**v1.0**

Table des matières

[1 Introduction 3](#_Toc484521530)

[1.1 Purpose of the document 3](#_Toc484521531)

[1.2 Other documents 3](#_Toc484521532)

[1.3 Compatibility warning 3](#_Toc484521533)

[1.4 Syntax used in the document 3](#_Toc484521534)

[1.5 Syntax used in MONARC 3](#_Toc484521535)

[2 Home page 4](#_Toc484521536)

[2.1 Dashboard 4](#_Toc484521537)

[2.2 Creating an Analysis 4](#_Toc484521538)

[2.3 Main analysis view 5](#_Toc484521539)

[3 Client Environment Administration 6](#_Toc484521540)

[3.1 Administration of users 6](#_Toc484521541)

[3.1.1 List of users 6](#_Toc484521542)

[3.1.2 User rights and information 7](#_Toc484521543)

[3.2 Managing the current user account 7](#_Toc484521544)

[4 Analysis management 8](#_Toc484521545)

[4.1 Method steps calls 8](#_Toc484521546)

[4.2 Library 9](#_Toc484521547)

[4.2.1 Organization of assets 9](#_Toc484521548)

[4.2.2 Asset Management 9](#_Toc484521549)

[4.2.3 Create an Asset 11](#_Toc484521550)

[4.2.4 Edit an asset 12](#_Toc484521551)

[4.2.5 Importing an asset 13](#_Toc484521552)

[4.2.6 Exporting an asset 14](#_Toc484521553)

[4.3 Information Risks 14](#_Toc484521554)

[4.3.1 Risks table 14](#_Toc484521555)

[4.3.2 Risk information sheet 16](#_Toc484521556)

[4.3.3 Adding additional risk 17](#_Toc484521557)

[4.3.4 Contextual menu 18](#_Toc484521558)

[4.3.5 Updating impacts and consequences 19](#_Toc484521559)

[4.4 Operational risks 19](#_Toc484521560)

[4.4.1 Risks table 19](#_Toc484521561)

[4.4.2 Operational risk sheet 20](#_Toc484521562)

[4.4.3 Adding additional risk 21](#_Toc484521563)

[5 Evaluation Scales 22](#_Toc484521564)

[5.1 Scale of impact 22](#_Toc484521565)

[5.2 Scales of threats 23](#_Toc484521566)

[5.3 Scales of vulnerabilities 23](#_Toc484521567)

[5.4 Management of operational risk acceptance thresholds 23](#_Toc484521568)

[6 Management of Knowledge base 24](#_Toc484521569)

[6.1 Type of assets 24](#_Toc484521570)

[6.2 Threats 24](#_Toc484521571)

[6.3 Vulnérabilities 25](#_Toc484521572)

[6.4 ISO 27002 controls 25](#_Toc484521573)

[6.5 Risks 25](#_Toc484521574)

[6.6 Tags (operational risks) 25](#_Toc484521575)

[6.7 Operational risks 25](#_Toc484521576)

[7 Gestion des interviews 26](#_Toc484521577)

[8 Snapshots 27](#_Toc484521578)

[9 Managing the implementation treatment plan 28](#_Toc484521579)

# fond_doc2fond_doc2fond_doc2Introduction

## Purpose of the document

The purpose of this document is to provide an exhaustive explanation of all the options in the MONARC tool.

## Other documents

“MONARC\_Quick-Start”: Provide a quick start with MONARC.

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

## Compatibility warning

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

## 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.

## Syntax used in MONARC

 : Button that always brings up the menu.

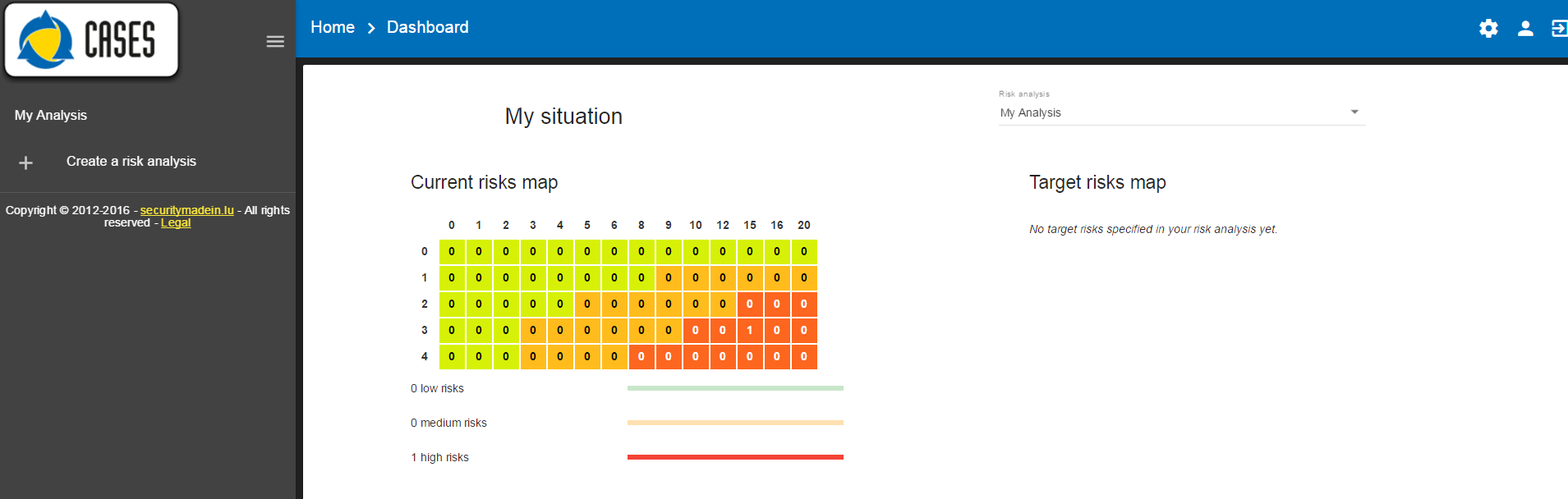
: Creating/adding something in context (assets, recommendations, etc.).

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

# Home page

## Dashboard

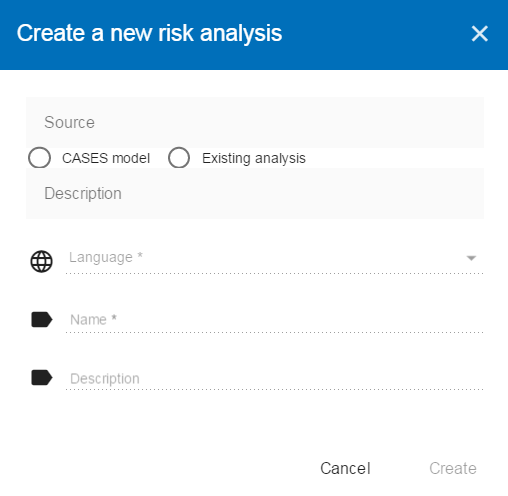
Immediately after user authentication, the following screen appears. It may, however, be slightly different, if there is not yet an analysis created or if there are already several and according to the state of progress of the analysis.



1. Graph showing the statistics of the last modified analysis.
2. List of existing analyzes. In this case, there is only one. Click on the analysis to select it (see chapter 2.3)
3. Click to create a new analysis (see chapter 2.2).
4. Navigation bar
5. Administration of the client environment. Click on "Manage account", "Manage users" or "Disconnect" (see chapter 3).

## Creating an Analysis

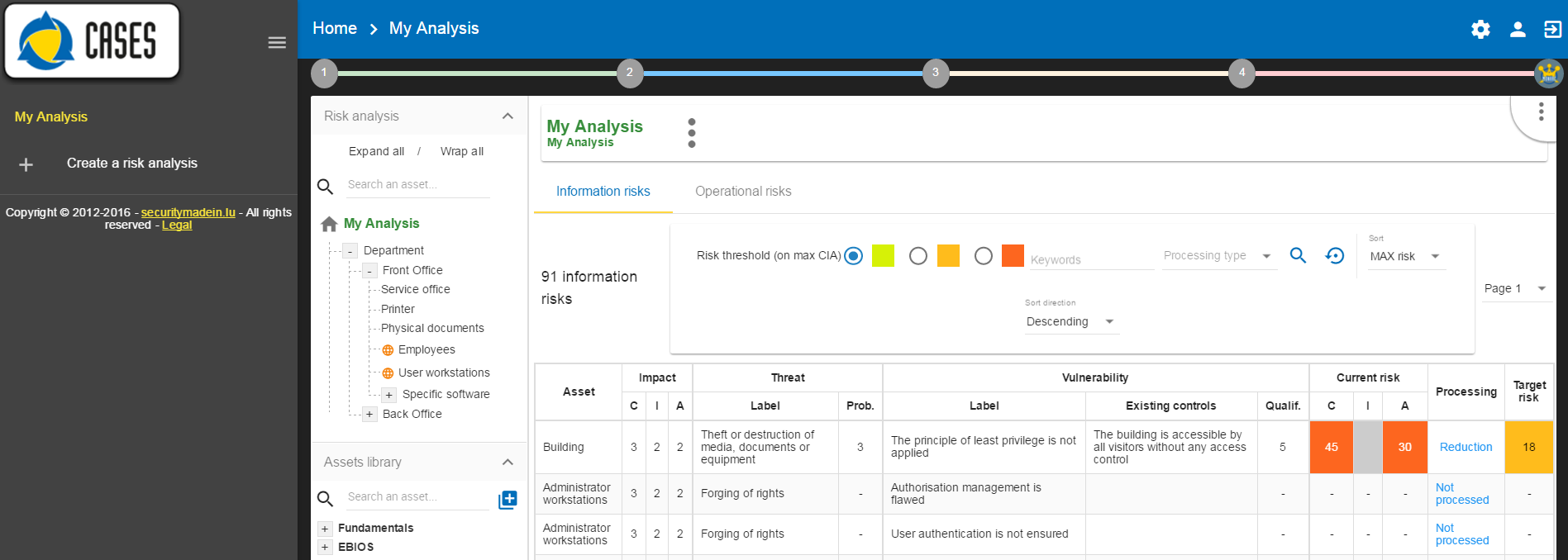
After clicking on "Create a Risk Analysis", the following pop-up appears:



1. The creation of an analysis is always based on an existing model. There are two choices for this:
   1. "CASES Model": Proposes available models in the knowledge bases. This option has at least two choices, "Modelling CASES", this is the default template made available by the MONARC editor. It provides sufficient knowledge bases to start an analysis. This option should be used by default to start a new analysis. There is also the choice "Blank model" which is a completely empty model. This template is typically used temporarily as a "Sandbox" to test the contents of an import xml file, for example.
   2. "Existing analysis"; Duplicate an analysis of your choice present in your environment.
2. Options a) or b) selected, select the source.
3. Select the preferred language for this new analysis. MONARC only present the languages actually available in the selected source.
4. Give your analysis a name.
5. Optional field, which allows you to describe your analysis in more detail.
6. If all required fields are filled in, click on "Create".

Once created, the analysis is selected by default.

## Main analysis view



*Once the analysis has been selected, the dashboard can be retracted in order to optimize the horizontal space by clicking on the symbol .*

# Client Environment Administration

There are two profiles:

* Administrator: Rights to create, modify, and delete users. An administrator does not have the access rights on the analysis (but he can give them).
* Users: Access right on analysis.

By risk analysis, there are 3 types of rights:

* No access rights (not even read).
* Read only.
* Read, write.

View of menus when you are an administrator:



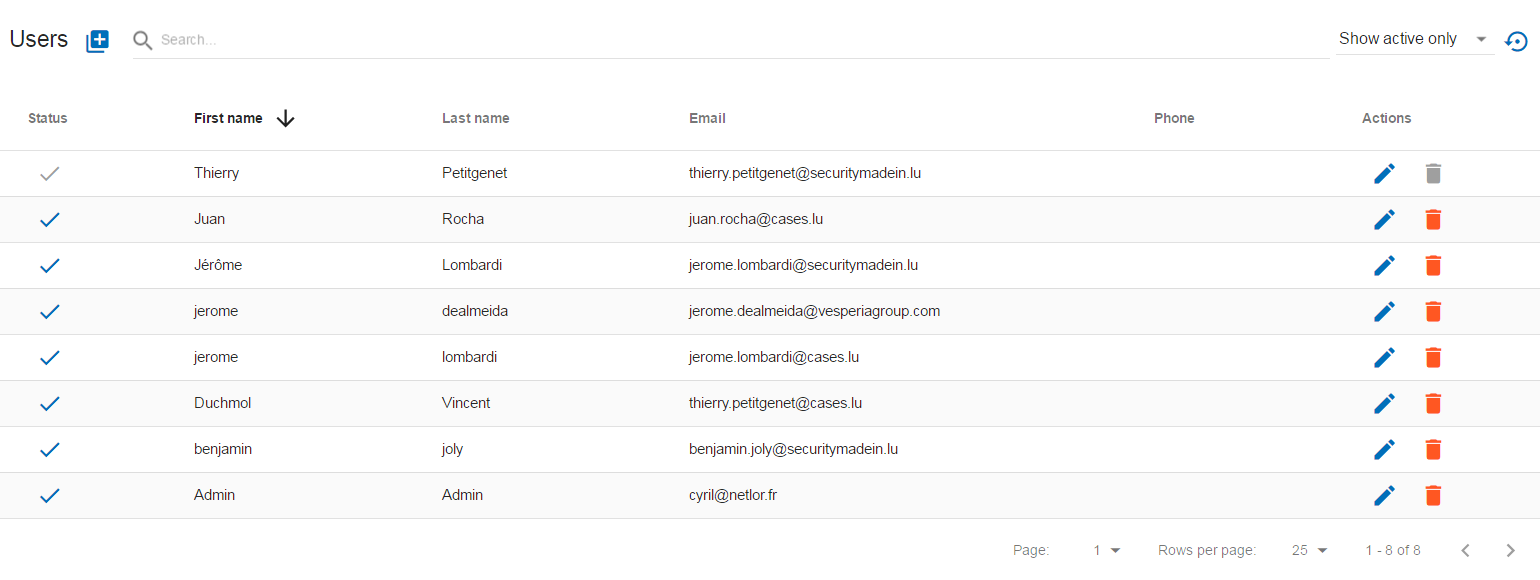
View of menus when you are a user:



1. User Administration (see chapter 3.1)
2. Managing the current user account (continued chapter 3.2)
3. Disconnection (closing of the MONARC session)

## Administration of users

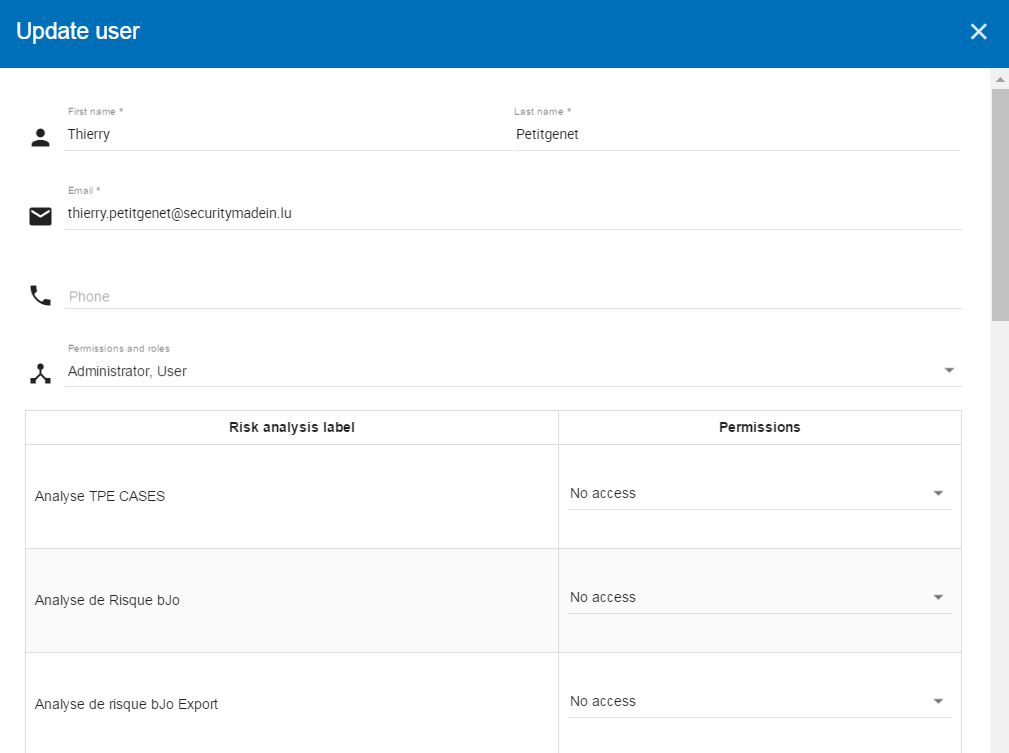
### List of users



1. Create a user or administrator.
2. Status: Activating or deactivating accounts.
3. Information about the person.
4. Editing a person's information.
5. Deleting a person.

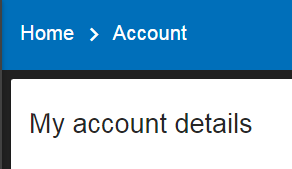
### User rights and information

After clicking the "" icon, the following screen appears:

1. General information.
2. Selection of profiles "Administrator" or "User".
3. Management of user rights by analysis.

## Managing the current user account

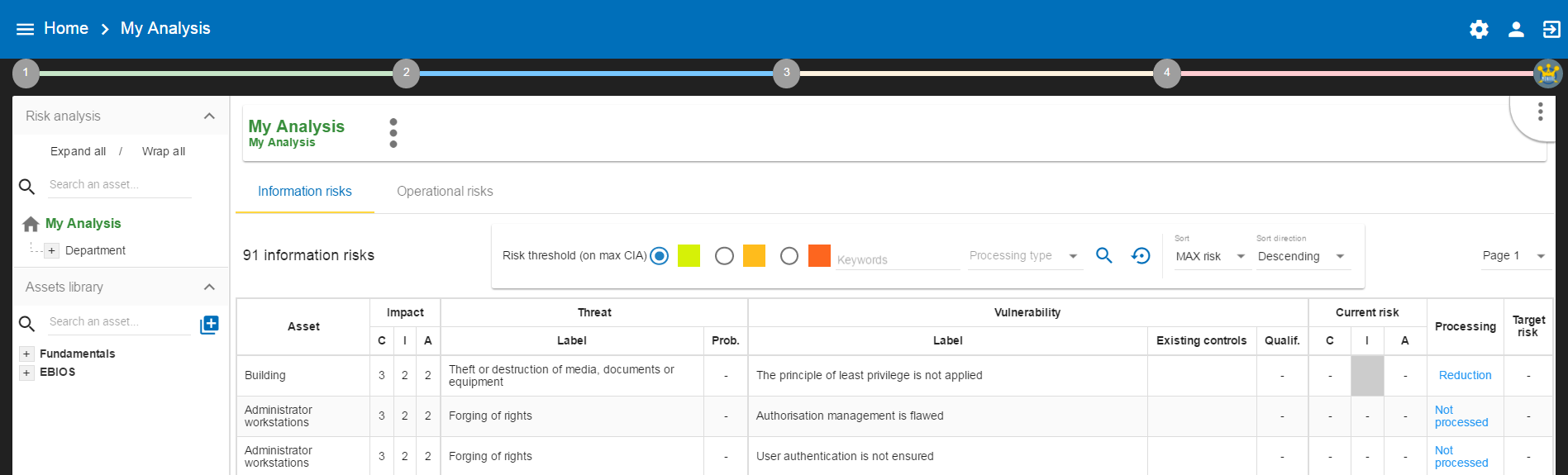


This view allows you to:

* Manage general user information.
* Change the password. Password complexity is required.
* Change the language of the consultation. This action only changes the language of the interfaces, the information specific to the data of the analysis remains in the same)
* Manage general information about the entity (MONARC account).

# Analysis management

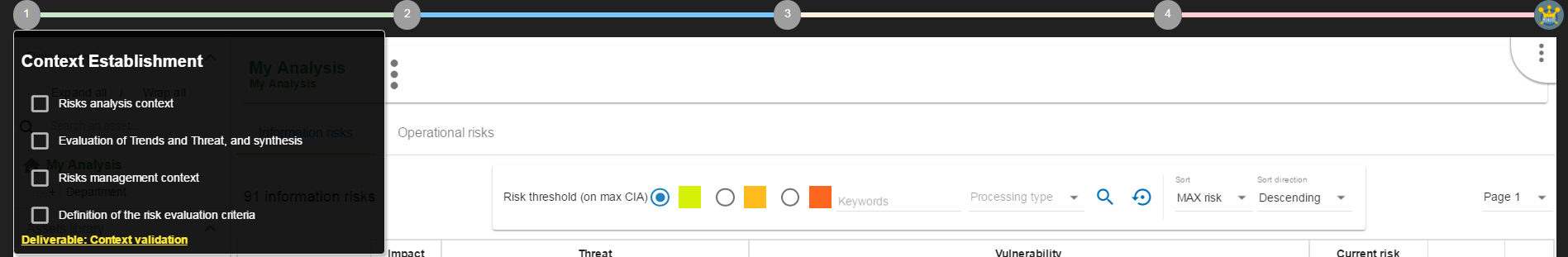
The main view of the analysis consists of 4 distinct parts.

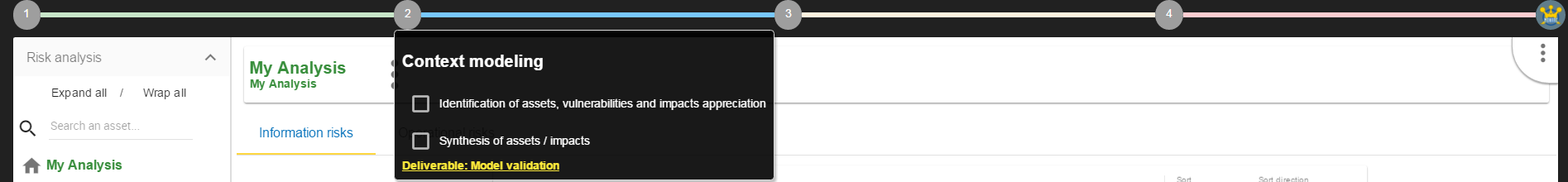
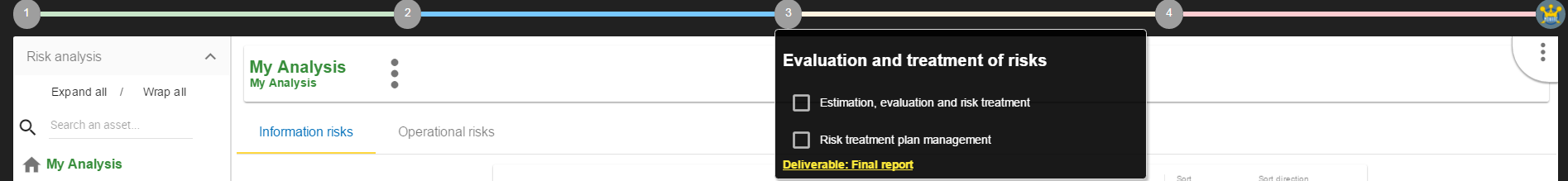
 

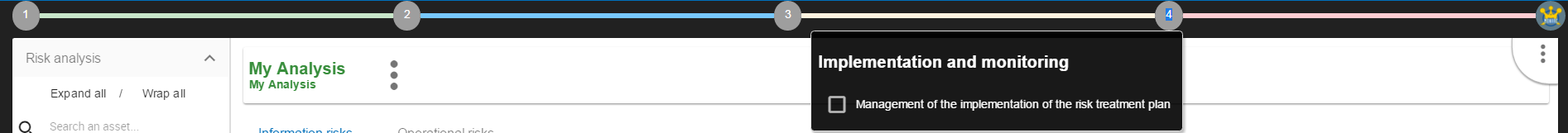
1. Access to the steps of the method: Click on the numbers from 1 to 4 to access the menus which follow the step-by-step method (see chapter 4.1).
2. Asset library area: Asset storage. The "drag-and-drop" function must be used to place these assets in the analysis just above 4.2).
3. "Risk Analysis" area: allows you to structure the assets of the analysis hierarchically by using the "Drag and Drop" function (hold down the left mouse button to move an asset). (Continued chapters 4.3 et 4.4)
4. Contextual area of work in the analysis: Depending on the assets and active parts of the analysis, this area contains contextual elements of the work.

## Method steps calls

By clicking on the numbers 1 to 4, a contextual menu appears.



1. Ticking the boxes change the progress of the method.
2. Click on the label, call the contextual management sub-screen.

## Library

### Organization of assets

Click on the "+" and the "-" to unfold and fold the categories of the library.

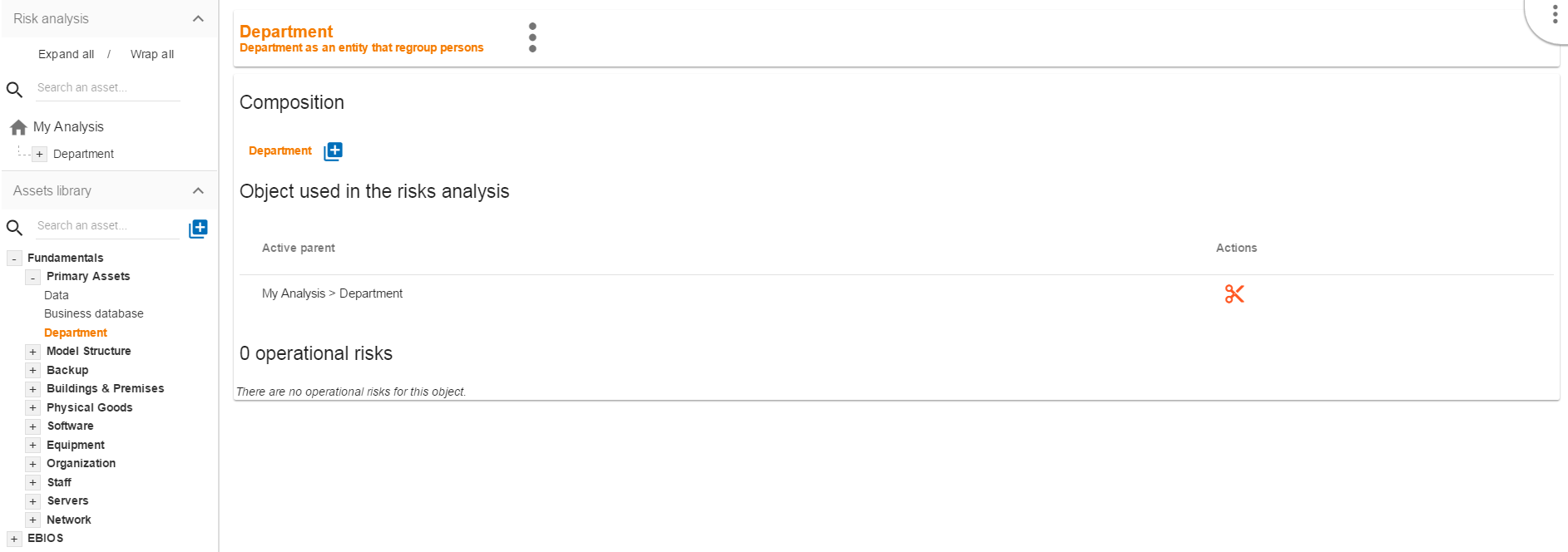
|  |  |
| --- | --- |
|  | 1. Search area in order to quickly find an asset. 2. Button for creating / importing assets (continued chapter 4.2.3). 3. The root level of the library. There are usually two:    1. "Fundamentals": Contains all default assets offered by CASES.    2. "EBIOS": Contains assets inspired by EBIOS. These are assets containing non-optimized risk models. 4. Conteneur secondaire permettant de classer les actifs par types logiques. 5. Asset level: These are the assets that must be "Drag and Drop" in the analysis. |

### Asset Management

The information on each asset is different depending on its type: "Primary" or "Secondary". This concept is explained in detail in Chapter 6.1 “Types of assets”.

#### Primary asset

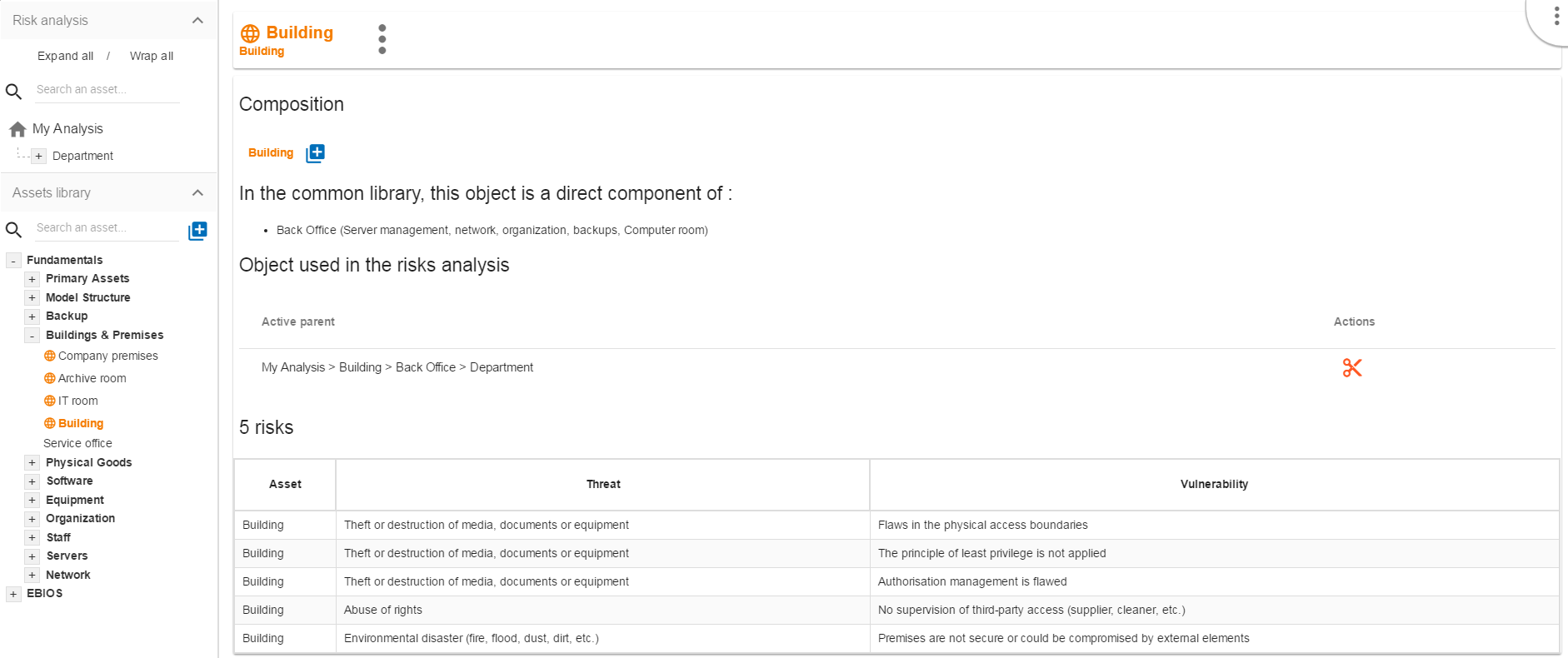
Click on a primary asset of the library, usually categorized in "Fundamentals \ Primary Assets".



1. Asset management context menu (details in chapter 4.2.2.3).
2. Add an existing asset in the structure, creating a composed asset. There is no limit in the asset tree.
3. Indication if this asset is currently used in the analysis. In this case, it is found at the root of the analysis.
4. Ability to detach asset from analysis. *Warning to completely detach an asset from the analysis will remove all its evaluation.*
5. Table of operational risks possibly associated with the asset. A primary asset cannot possess information security risks. The modification of the operational risk table is based on the knowledge base.

#### Secondary assets

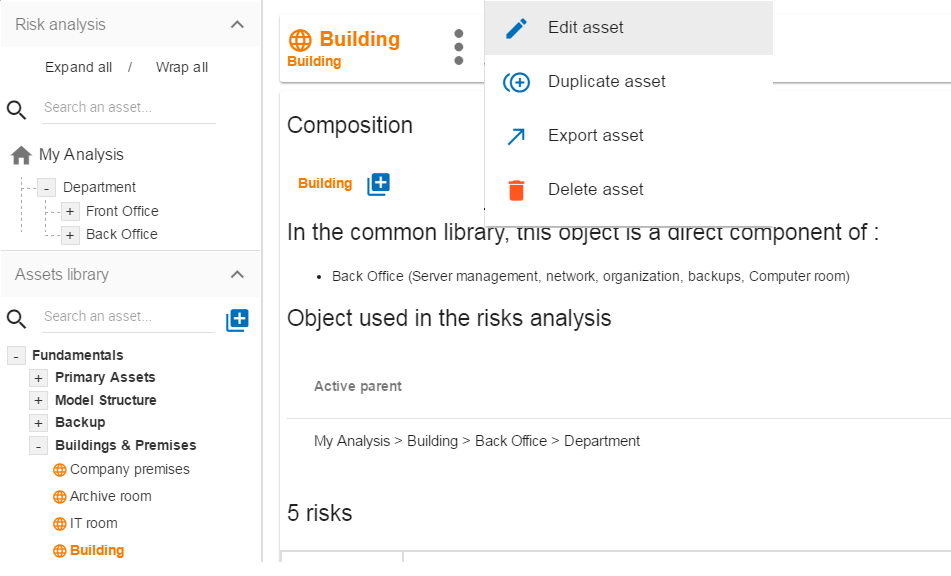
Click on a secondary asset of the library, for example on «Building» classified in «Fondamentaux \ Bâtiments & locaux».



1. Asset management context menu (details in chapter 4.2.2.3).
2. Add an existing asset in the structure, creating a compound asset. There is no limit in the asset tree.
3. Indication if the asset is already part of the composition of another asset. In case, it is already a sub-element of the assets "Back Office".
4. Indication if this asset is currently used in the analysis. In this case, it is found at the 3rd level of the root of the analysis.
5. Ability to detach asset from analysis. *Warning to completely detach an asset from the analysis will remove all its evaluation.*
6. Risk information table associated with the asset. Conversely, in the case of primary assets, media assets can only have information risks. The risk table is modified from the knowledge base.

#### Context menu

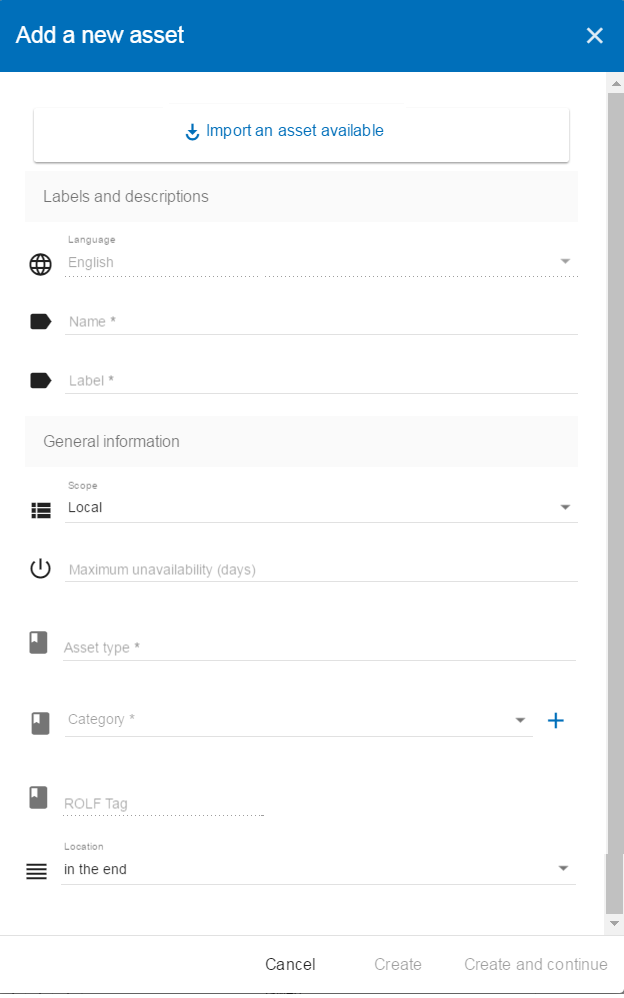
By clicking on the "" icon, the following context menu appears. Whatever the asset type of the library, the menu is the same.



1. Adds an existing asset to the structure, creating a compound asset.
2. Starts the pop-up that allows you to modify most of the parameters of an asset (see chapter 4.2.4).
3. Create a copy of the asset named "Name (copy # 1)", which is then renamed with the "Edit Asset" option.
4. Launches asset export pop-up (continued chapter 4.2.6).
5. Deletes an asset. Caution, this action is definitive, even if the asset is used in the analysis.

### Create an Asset

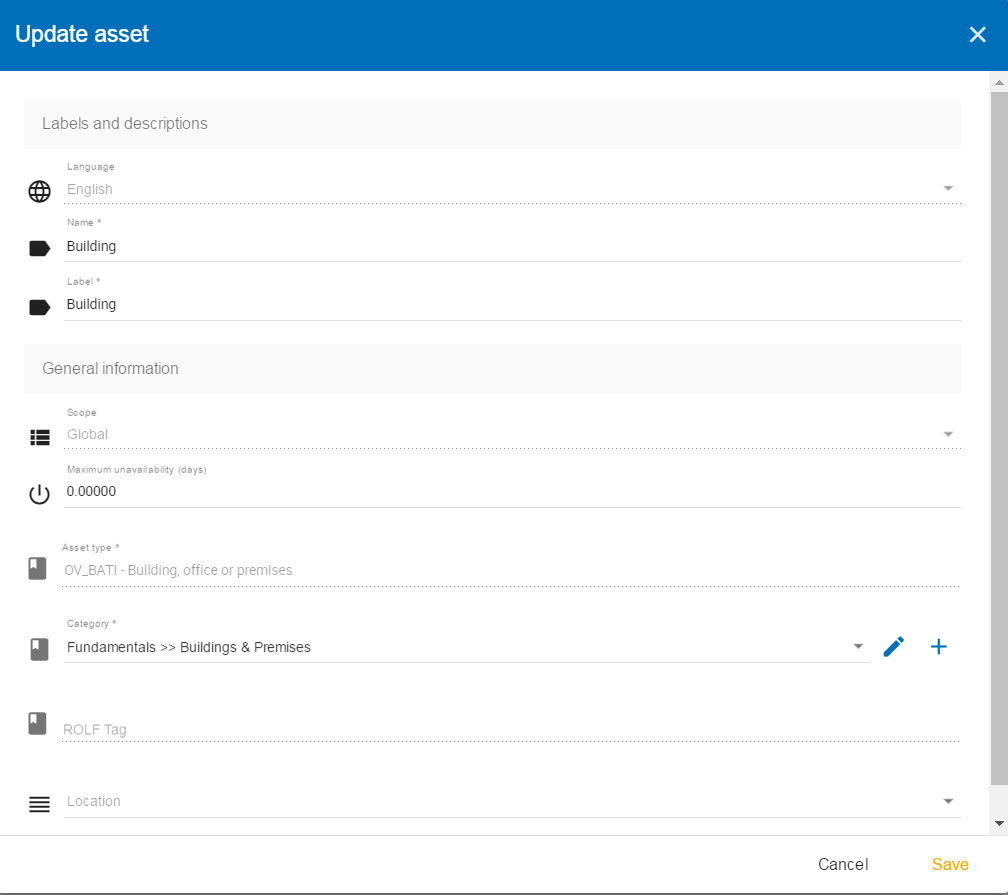
In the library, after clicking on "Add Asset", the following pop-up appears:



1. To create an asset, it is also possible to import it (see chapter 4.2.5).
2. Language selection: This option cannot be used, the default language of the analysis is imposed.
3. Asset Name: This name must be unique for the analysis.
4. Asset label: This is an additional description, it is displayed in the tooltip when the mouse is positioned without moving on the asset.
5. Scope of the asset, two possible choices:
   1. Local: Identified asset risks are to be assessed whenever the asset is present in the analysis. A primary asset is generally local in scope.
   2. Overall: the identified risks of the asset are only to be assessed once for the whole analysis. This option is to be used mainly for the support assets, as soon as they are included in several primary assets. Example, the computer room, the main building: once the risks assessed only the impact from the primary asset can change the level of risk.
6. Optional information indicating the unavailability period beyond which the impact on the body becomes significant or greater. The collection of this information makes it possible to compare the business requirements (primary assets) with the resilience of all the support assets.
7. Selection of the type of asset: It determines the nature of the asset and therefore the risk model associated with it.
8. Select the category, ie the location in the library where the asset will be stored, or create a new category.
9. For primary assets only, the "Operational Risk Group" allows the asset to be associated with operational risks by default.
10. Allows you to order assets in the selected category.

### Edit an asset

The call is made from the context menu when a library object is selected. The following pop-up appears:

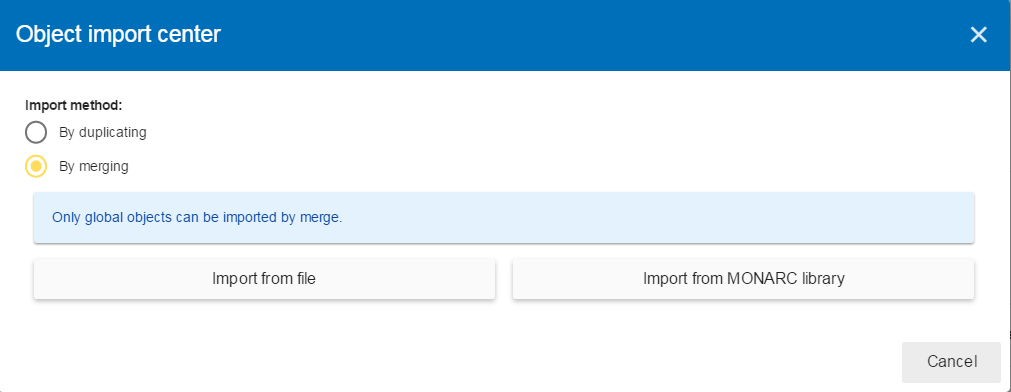


For an explanation of all the fields that can be changed, see section 4.2.3 "Creating an Asset". For technical reasons, the modification does not make it possible to modify:

* The selection of the language.
* The "Local" and "Global" scope of an asset.
* The operational risk group.

### Importing an asset

This pop-up is accessible from the pop-up "Add a new asset".

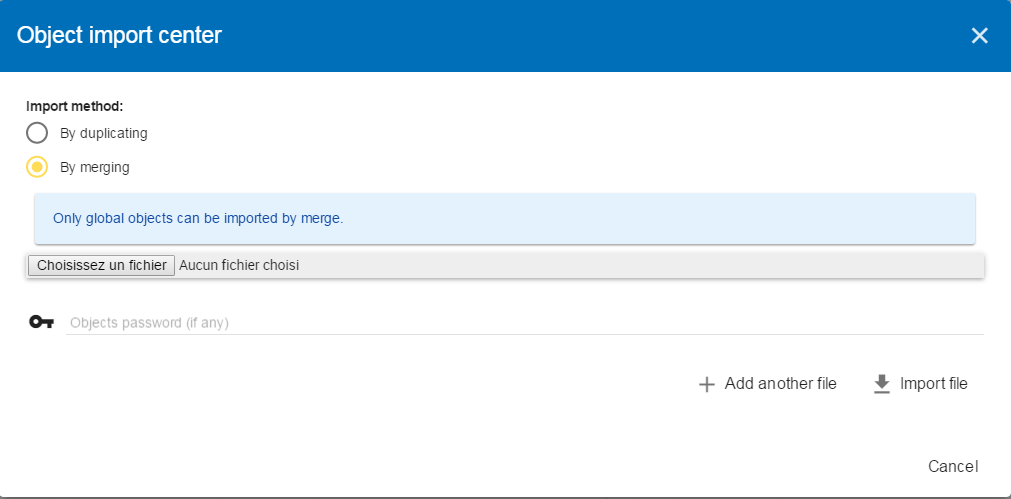
1. The import principle requires that the imported object remain in the category in which it is located. Two import methods are possible:
   1. "Duplicate": When importing, if an object of the same name exists, then it will be duplicated and the name will suffix "- Imp #n".
   2. "By merge": When importing, if an object of the same name exists, then it will be replaced. In this case, only the associated risk model will be modified.

*The import of an uncontrolled object can be destructive for the current analysis. It is strongly advised to create a Snapshot before importing, or to use an empty "Sandbox" analysis.*

1. "Import from file": allows to exchange assets from one environment to another (see chapter 4.2.5.1).
2. "Import from the MONARC library" ": This option is not available in the case of a" Stand alone "version of MONARC (see chapter 4.2.5.2).

#### Importing an asset from a file

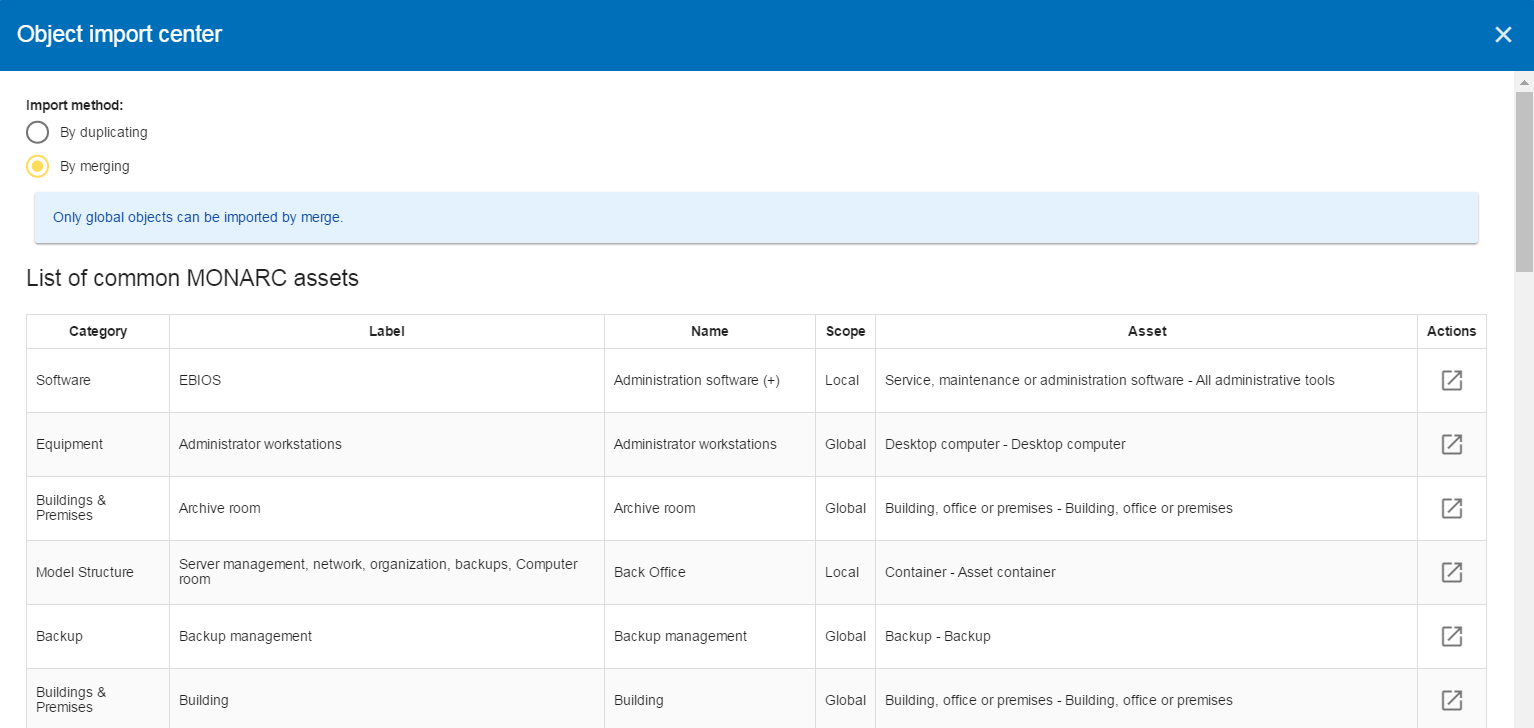
The pop-up appears after clicking on the "Import from File" option in the Asset Import Center.

1. Access the directories of the computer to point to a file.
2. Passwords: When exporting the selected file, a password has been used to encrypt the file, it must be entered here.
3. Starts importing file

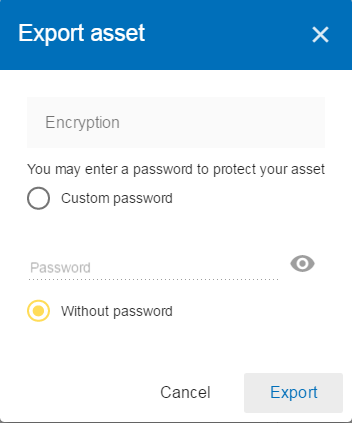
#### Import from the MONARC library

The pop-up appears after clicking on the "Import From File" option in the Asset Import Center.

**** 

1. Table of available assets in the common base.
2. Action: Initiate the import procedure for the corresponding asset.

### Exporting an asset

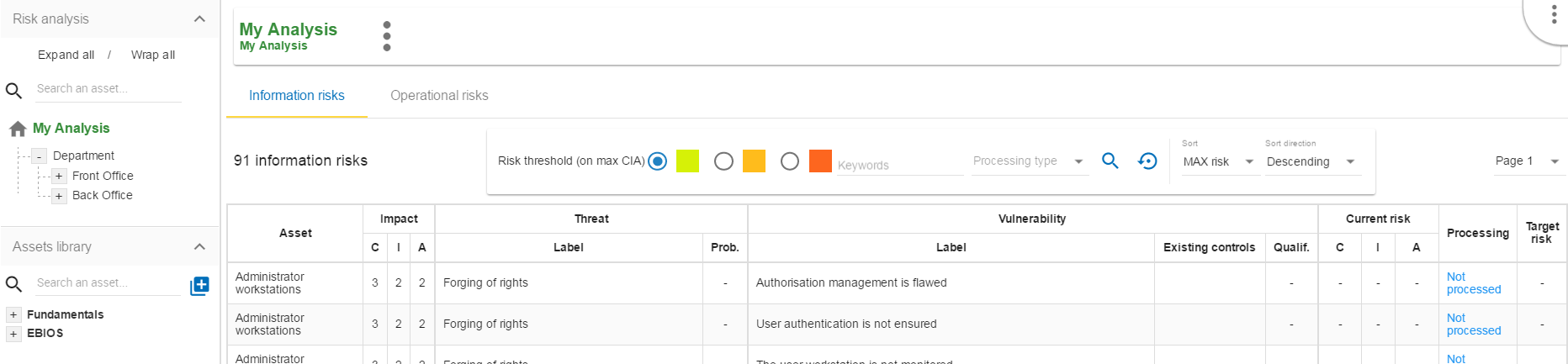
**** 

1. Possibility to encrypt the generated file with a symmetric password that will be necessary during the import.

## Information Risks

### Risks table

By selecting the top of the analysis or an asset in the tree, the risk table appears.

****

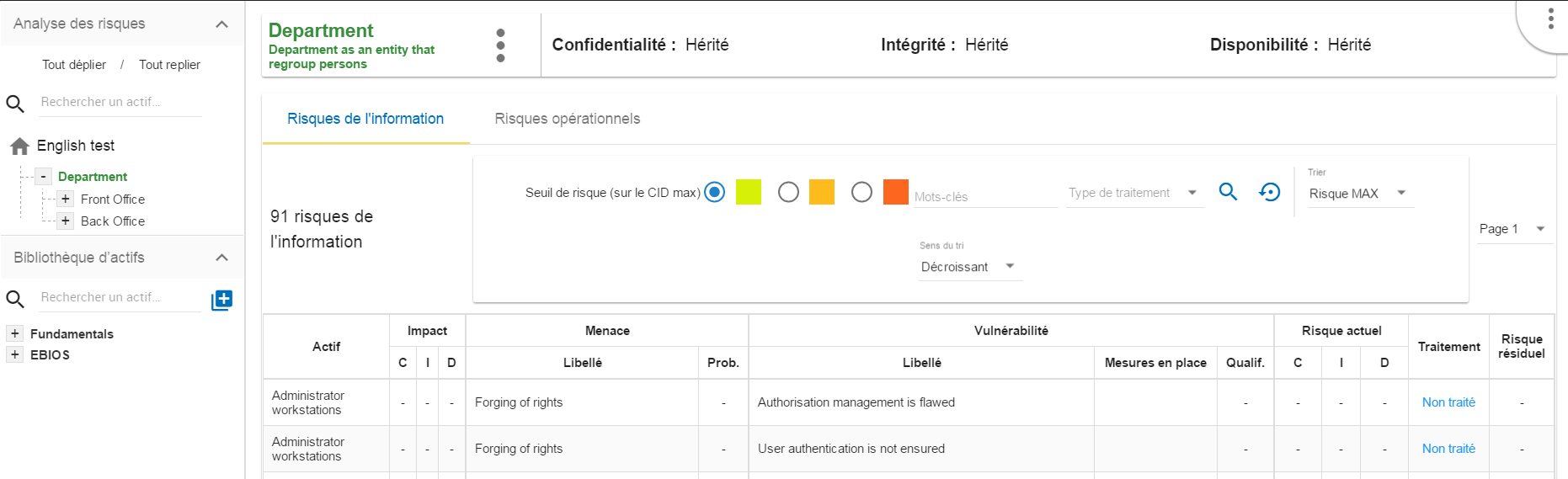
1. There are two separate risk tables:
   1. The information risk table based on CIA criteria.
   2. The operational risk table based on ROLFP

There are two business rules for managing the display:

1. Only supporting assets may have information risks.
2. Only primary assets may have operational risks.

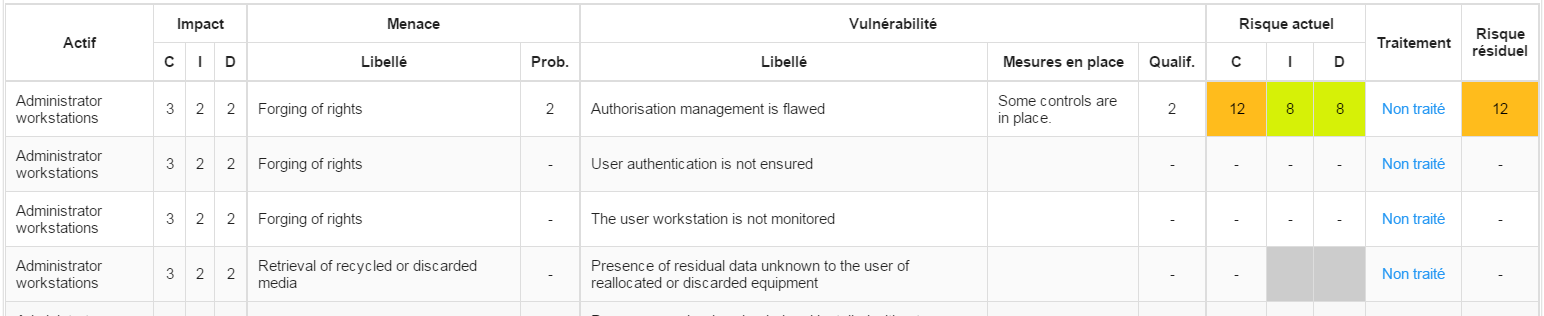
Depending on the asset being selected, the display may change:

* In the case of a primary asset:
  + There may be operational risks
  + The information risk table is composed of all the risks of the supporting assets of which it is composed.
* In the case of a supporting asset:
  + The information risk table is composed of all the risks of the selected asset.
  + The operational risk table does not exist.
* If the root of the analysis is selected:
  + The information risk table is composed of all the risks of the supporting assets that make up the analysis.
  + The operational risk table is composed of all the risks of the primary assets that make up the analysis.

1. The primary asset "Department" is selected in the analysis.
2. Display the CID impacts of the "Department".
3. Information Risk tab selected.
4. The "Department" asset consists of supporting assets that provide a total of 91 risks (in this example).
5. Possibility to select only certain risks according to the risk acceptance threshold.
6. Ability to sort on most columns of the table.
7. Selection of the page in the list of results.



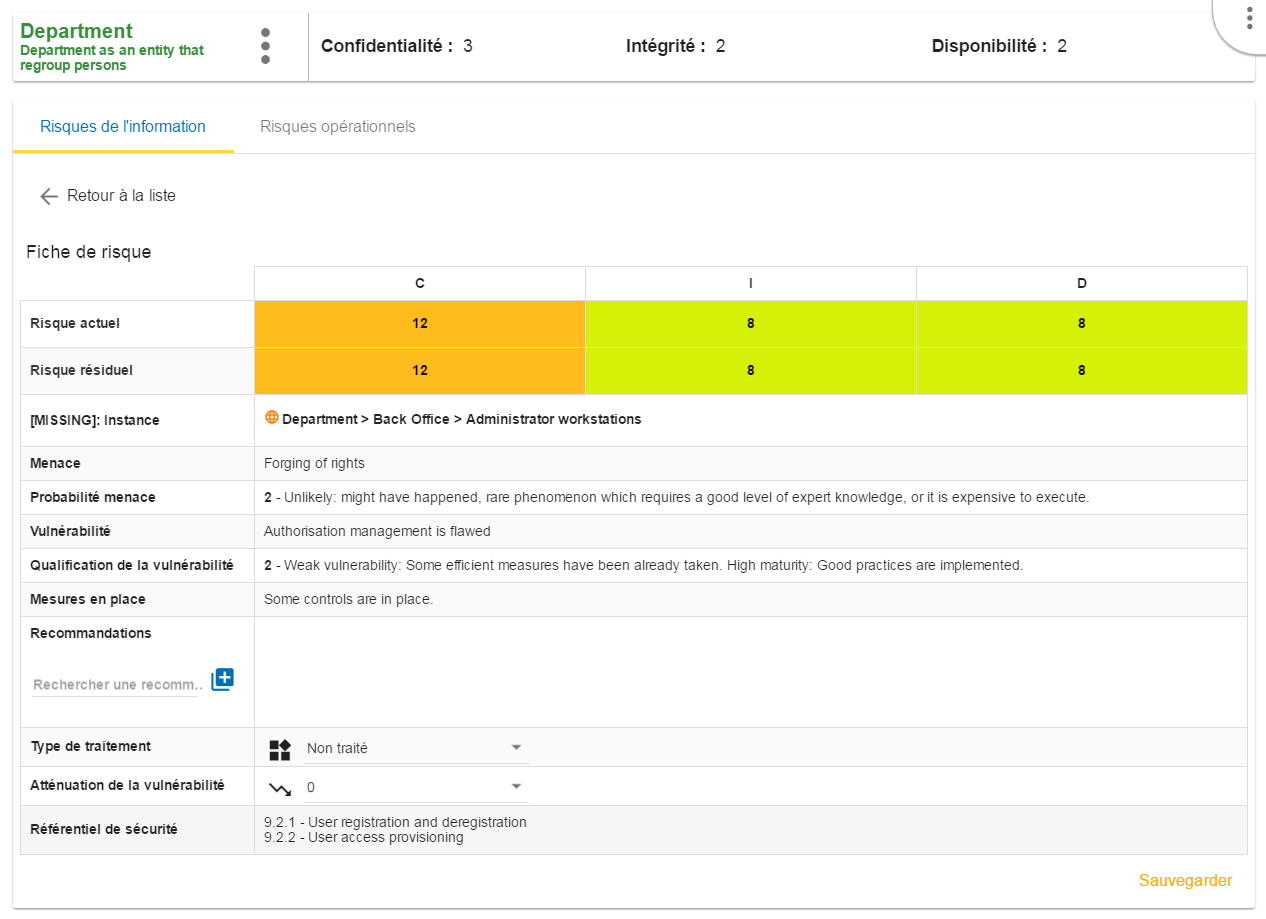


1. Assets involved in the evaluation.
2. The CIA criteria that have been assigned to the "Department" are inherited by default from the supporting assets.
3. Threat label.
4. Likelihood of threat (scales of assessment, see chapter 5).
5. Vulnerability label.
6. Control in place: Describe, in a factual manner, the security control in place concerning the vulnerability or, more broadly, the risk.
7. Evaluation of the control in place in order to determine the level of vulnerability (scales of evaluation, see chapter 5).
8. Risk value calculated according to the risk calculation formula. The colors depend on the risk acceptance grid (Risk acceptance grid, see chapter 5).
9. Indication if the risk is treated, and link to the risk profile (see chapter 4.3.2).
10. Value of residual risk. In the case of the figure above, the residual risk is equal to the max risk because it is not yet treated.

*By leaving the mouse on most fields, a help bubble appears after 1 second.*

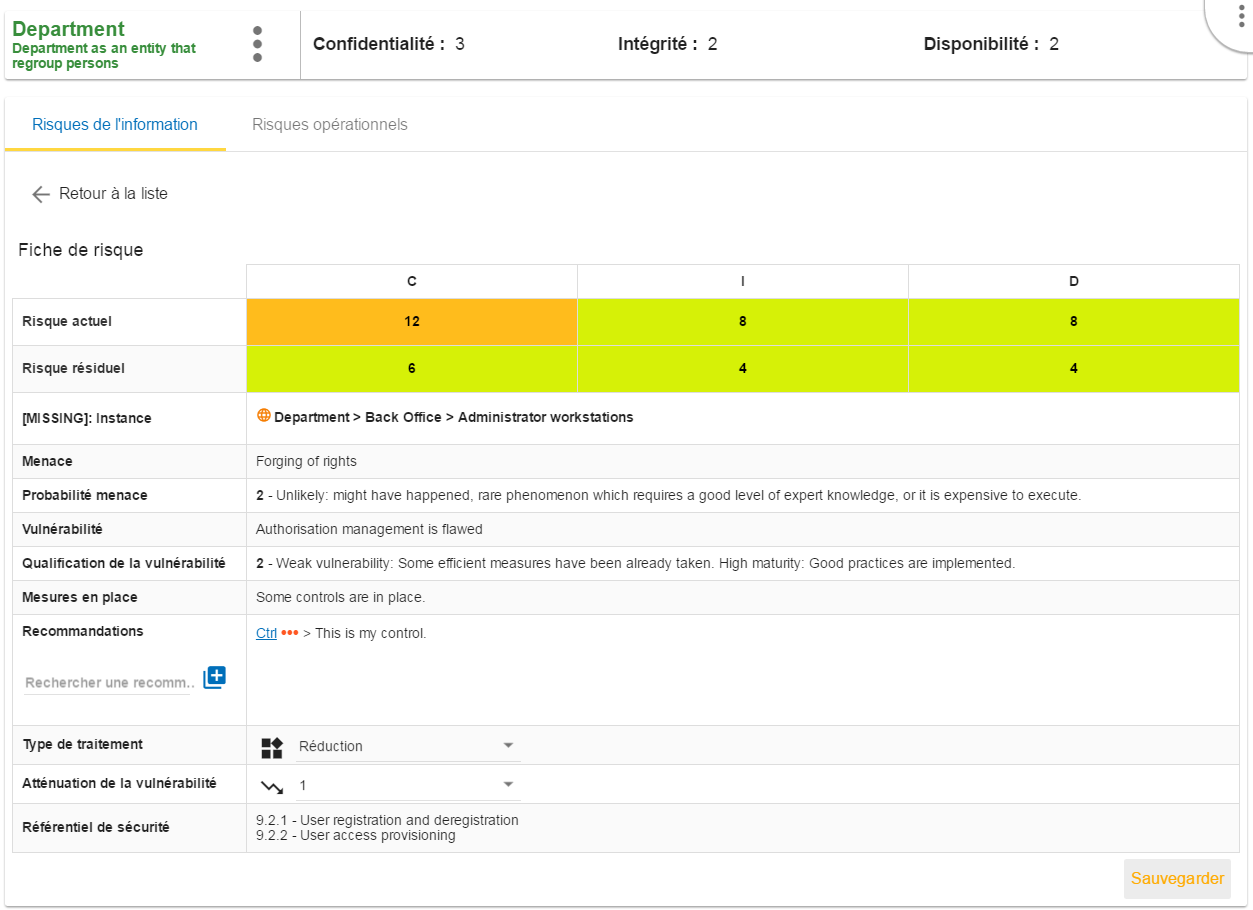
### Risk information sheet

The risk sheet is displayed when you click on the "Processing" link in the information risk table.

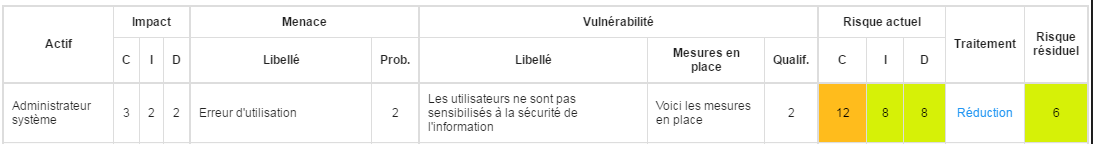


1. Click to turn back to risk table.
2. Risk values for CID criteria (not yet covered in the example).
3. Reminder of the parameters of the risk table.
4. Creation / Assignment button for one or more control(s).
5. Selection of the type of risk treatment, the 4 values have their sources of ISO / IEC 27005 :
   1. Modification / Reduce
   2. Refused
   3. Accepted
   4. Shared
6. Choosing a risk reduction value, the more effective the control is, the greater the reduction value is.
7. Proposal of controls which come from various repositories.
8. Saving the form in order to calculate the residual risk.

The figure above shows the risk profile after risk treatment and validation.

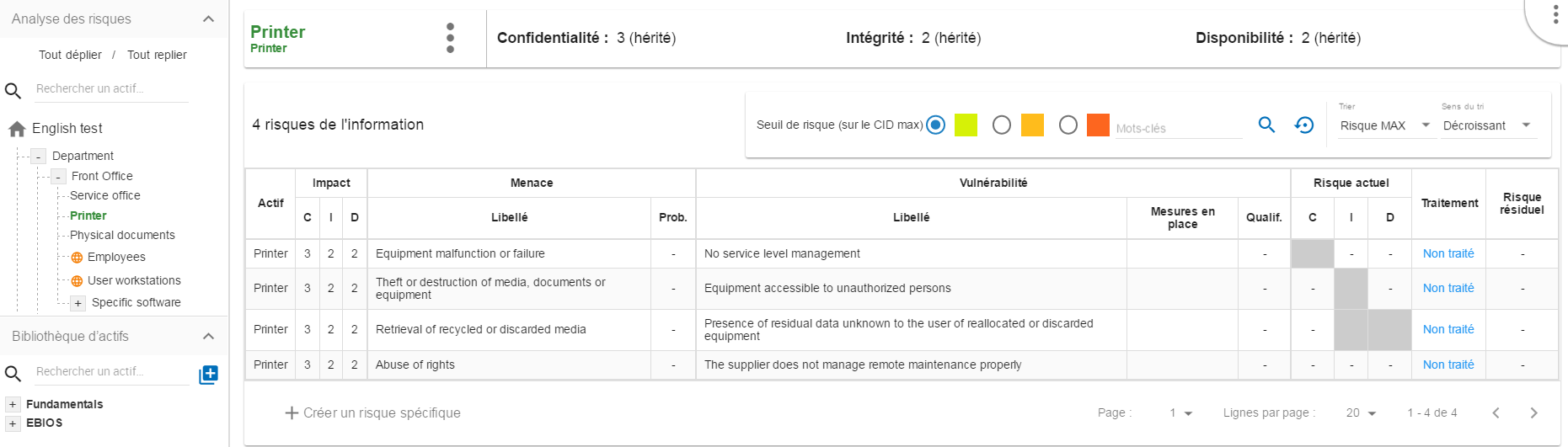


The risk table becomes:



### Adding additional risk

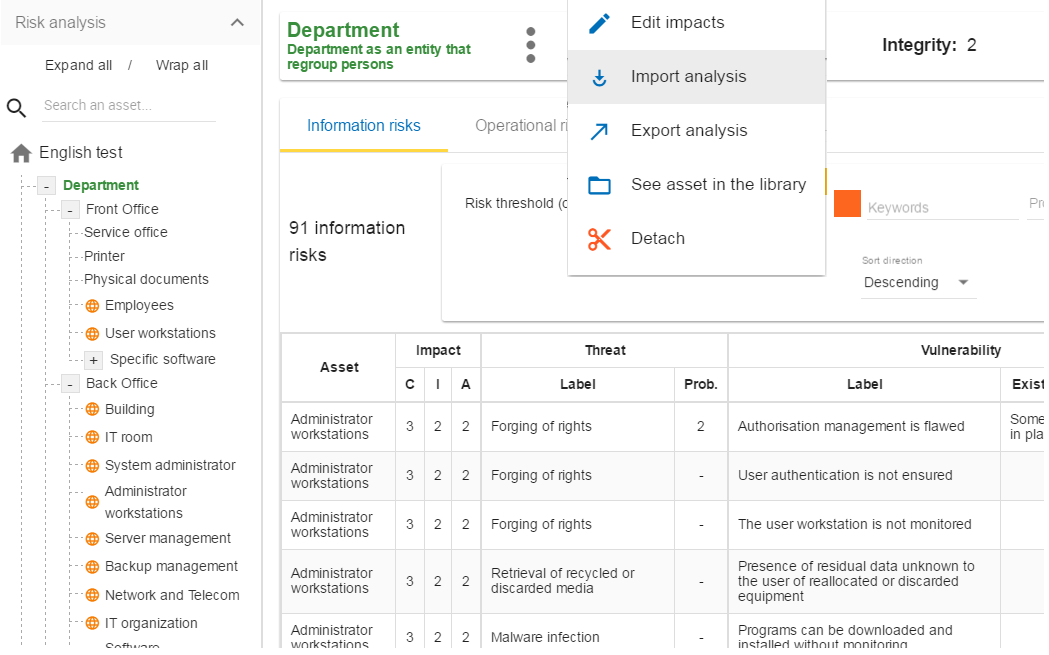
When an asset is selected in the analysis:

1. 1) Click to create a specific risk: A pop-up appears and allows to associate a threat / vulnerability pair with the current asset. Threat and vulnerability must exist beforehand.

### Contextual menu

By clicking on the 3 points, the context menu appears:

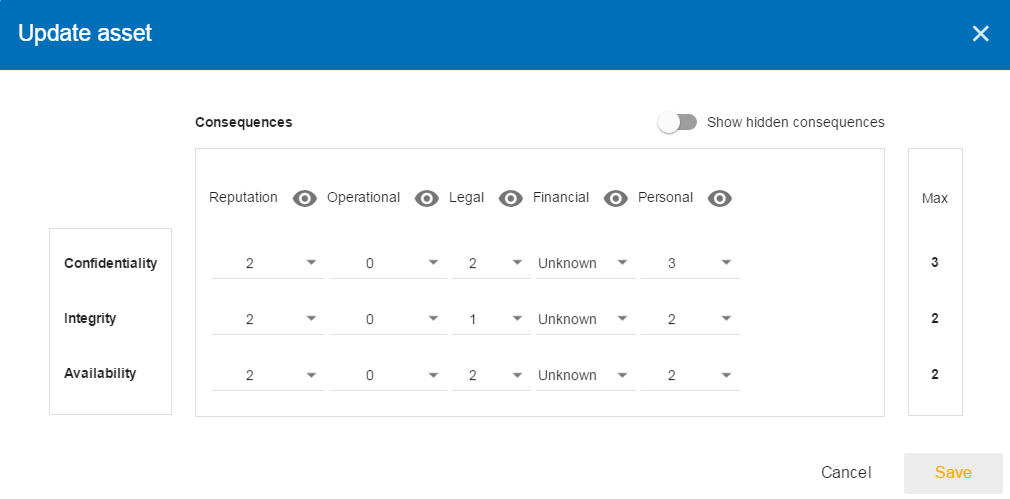


1. Displays the impact and consequence modification view (see chapter 4.3.5).
2. Allows you to import an analysis from the location pointed to by the selected asset of the scan. The import works exactly like importing an asset, see chapter 4.2.5).
3. Displays the asset from the library, allowing you to have another context menu that allows changes to the asset.
4. Allows you to export an analysis, from the place pointed by the selected asset of the analysis. The export works exactly like importing an asset, see chapter 4.2.6).
5. Detach removes an asset from the risk analysis. Caution this action may lead to the loss of risk assessments for this asset and its children*.*

### Updating impacts and consequences

The aim is to define the level of the primary assets the impacts and consequences that can result from the realization of the risks of the model.

The pop-up below appears:

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

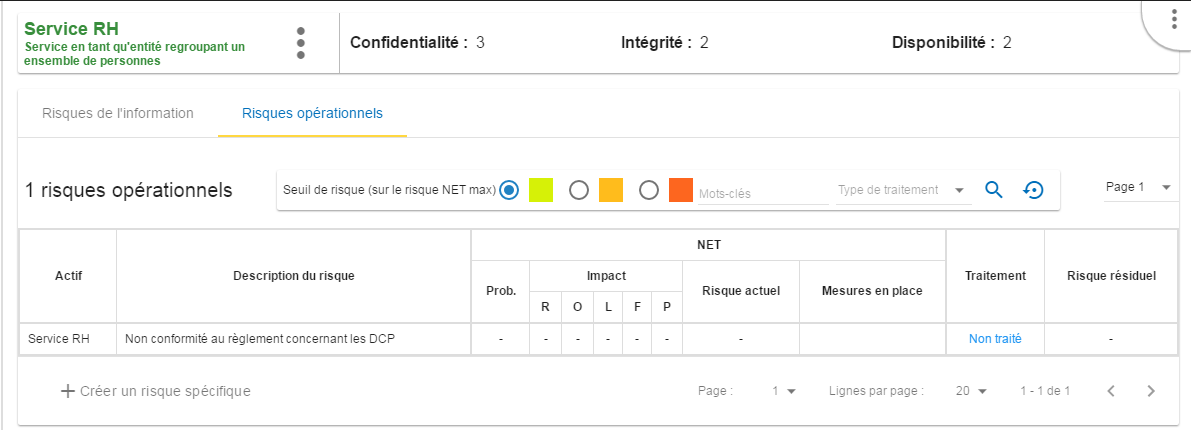
*By leaving the pointer unmoved over the numbers, the meaning of this number appears after one second.*

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 “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.

## Operational risks

### Risks table

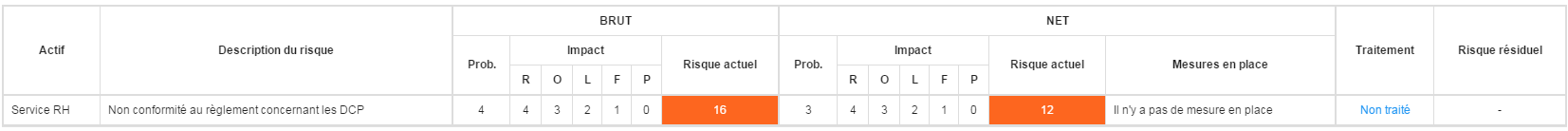


1. The primary asset "Department" is selected in the analysis.
2. The tab "Operational risks" is selected.
3. The asset "Department" has only one operational risk.
4. Ability to select only certain risks, according to the risk acceptance threshold.
5. Ability to sort on most columns of the table.
6. Selection of the page in the list of results.

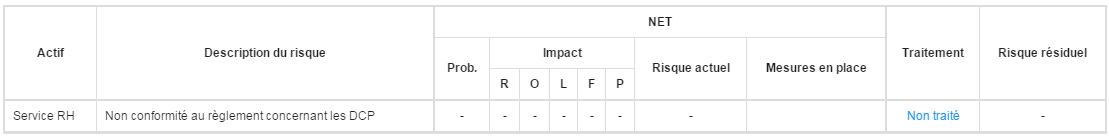
Depending on the option chosen, the operational risk table may or may not display the raw risks, ie risks that would impact the organization without any controls in place.

Some companies do not use this option, so to gain horizontal space, the risk part is hidden.





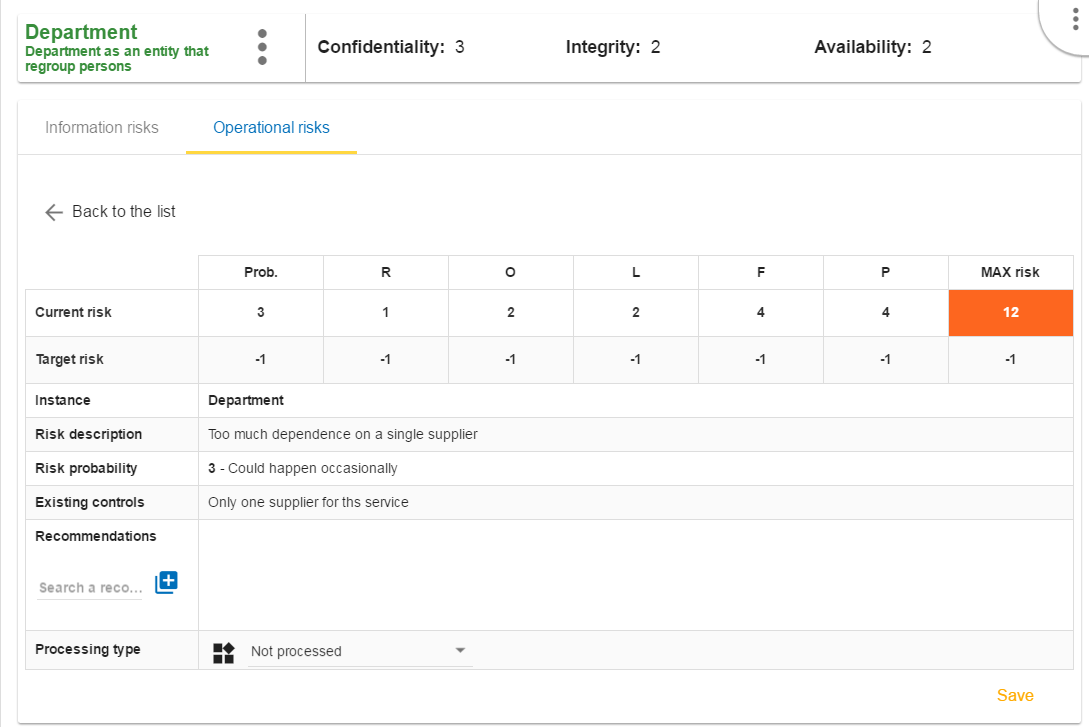




1. Assets involved in the evaluation
2. Description of risk
3. Raw operational risk is calculated from the two factors, the "probability" of the risk scenario and the impact based on the ROLFP (see rating scales in Chapter 5). The current risk represents the maximum value of the probability on the ROLFP impact values.
4. The NET risk represents the risk with the measures currently in place. The calculation is the same as for the raw risks.
5. Control in place: Describe here, in a factual manner, the control in place.
6. Indication if the risk is treated and risk profile (see chapter 4.4.2).
7. Value of the residual risk. In the case of the figure above, the residual risk is equal to the max risk because it has been not yet treated.

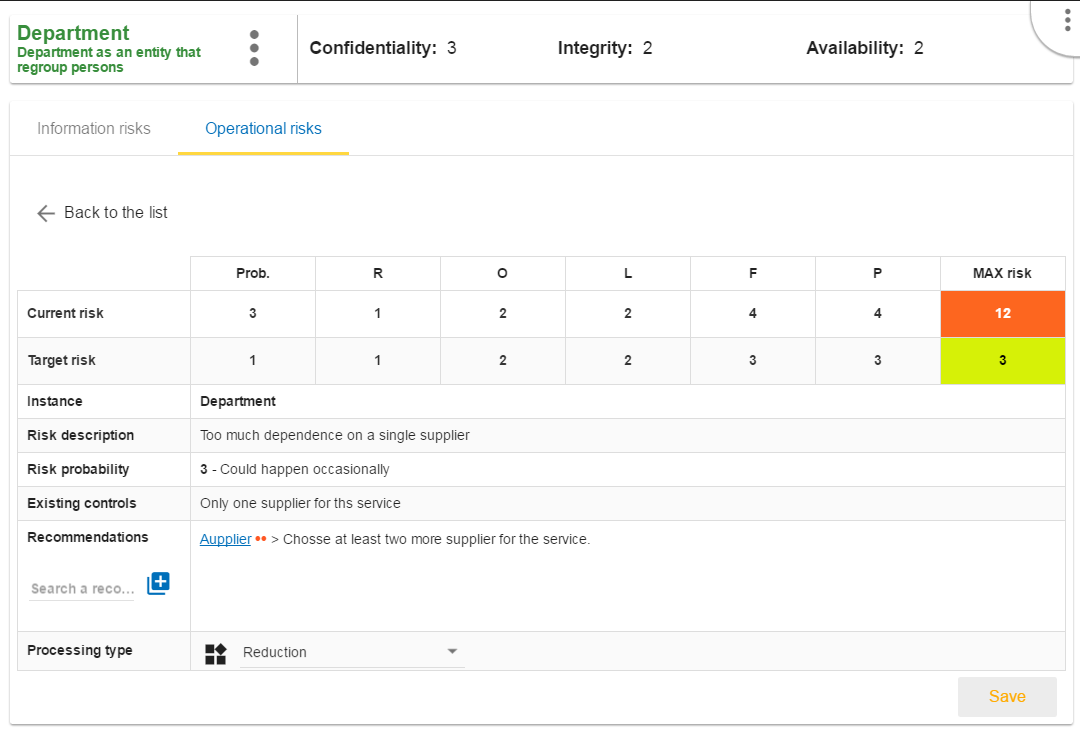
### Operational risk sheet

The risk card is displayed when you click on the "Processing" link in the information risk table.



1. Return to risk table.
2. Current Risk Values for ROLFP Criteria.
3. Residual risk values for the ROLFP criteria (not yet treated). These values should be adjusted according to the recommendation and the measures that will be put in place.
4. Reminder of the parameters of the risk table.
5. Creation / Assignment button for adding one or more control(s).
6. Selection of the type of risk treatment, the 4 values have their sources of ISO / IEC 27005 :
   1. Modification / Reduce
   2. Refused
   3. Accepted
   4. Shared
7. Saving the form in order to calculate the residual risk

Once the validation has been done, the risk is treated:



### Adding additional risk

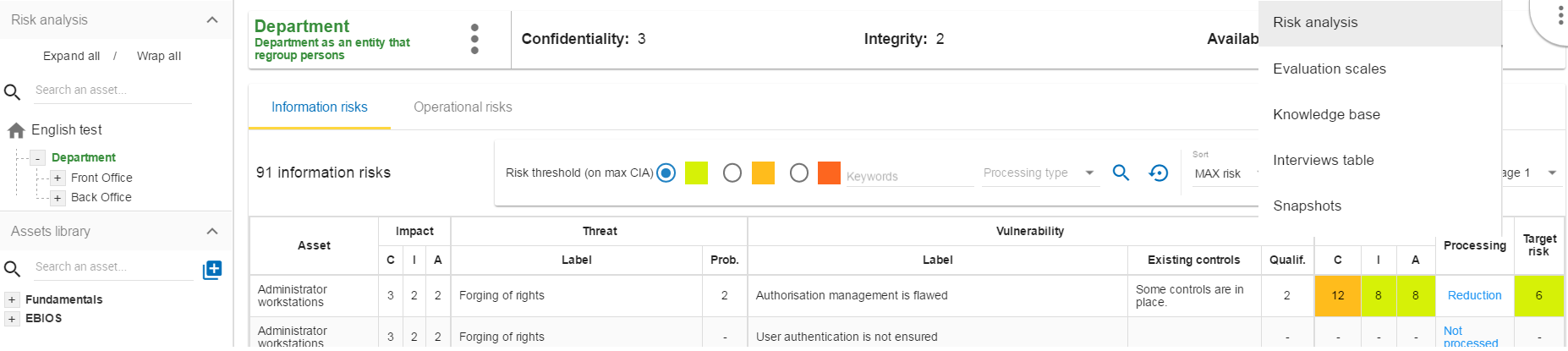
When an asset is selected in the analysis:

1. Click to create a specific risk: A pop-up appears and allows a new risk to be associated with the current asset. If the risk does not exist, it can be created directly.

# Evaluation Scales

The menu is always accessible from the main view of MONARC:



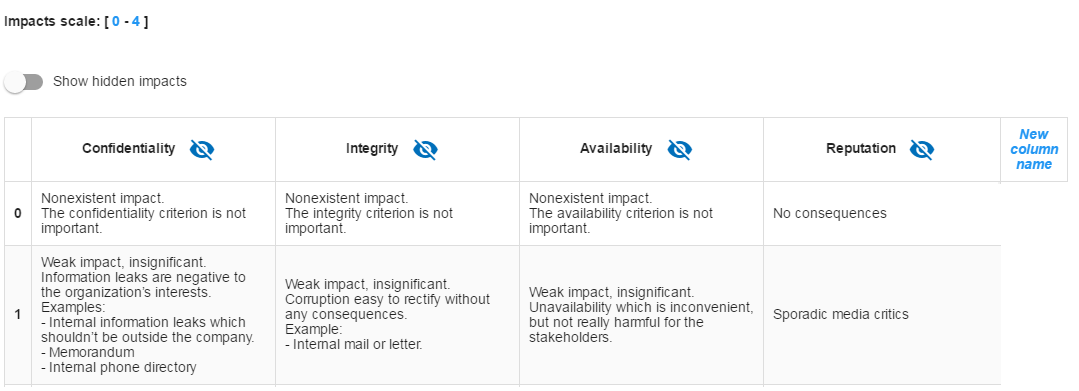
1. Calling the menu
2. Calling the Management view of evaluation scales

The view "Scales of Evaluations" shows the followinf criterias:

1. Scale of impact
2. Scale of threats
3. Scale of vulnerability
4. The management of information risk acceptance thresholds
5. The management of operational risk acceptance thresholds

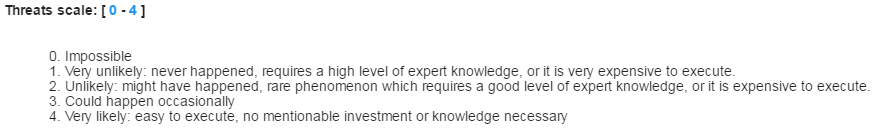
Note: All scales are editable and customizable. However, it is no longer permitted to modify scales as soon as an evaluation has been encoded.

## Scale of impact



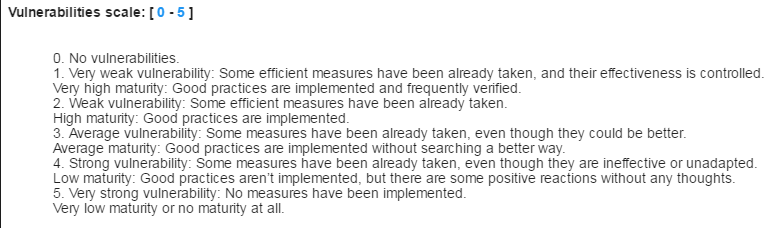
1. Click to change the number of steps.
2. Click to "Show or Hide" the unused criteria of the analysis.
3. Click on the symbol  to hide an unused column.
4. Click to add a new impact criterion.
5. Click to edit the labels of each step (management is such an Excel table, clicking on a label in order to edit it, by clicking on another, makes the first automatically saves and so on).

## Scales of threats



1. Click to change the number of steps
2. Click to edit the labels of each echelon (Management is same as scale of impact).

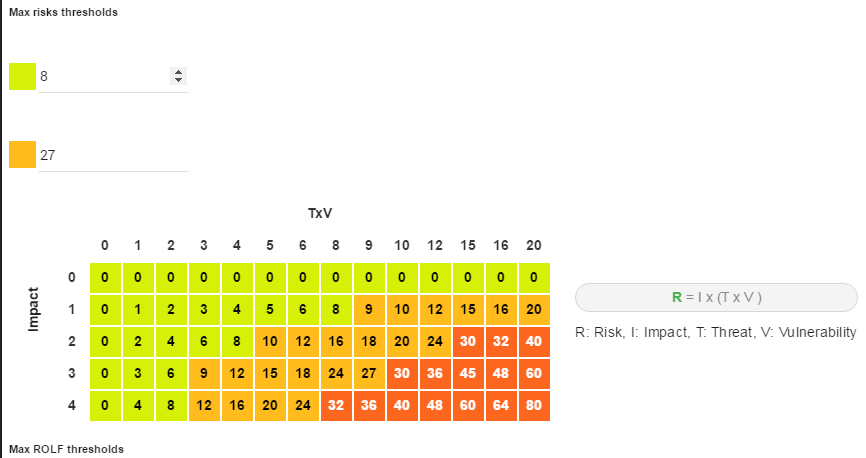
## Scales of vulnerabilities



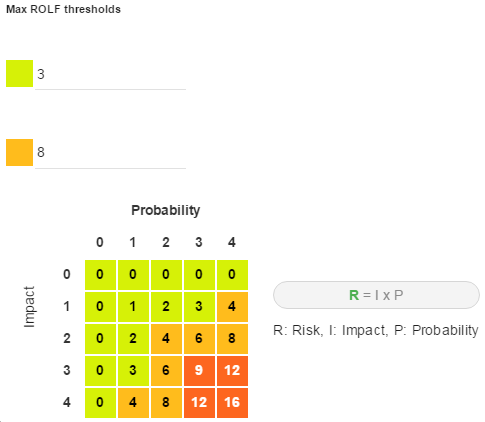
1. Click to change the number of steps
2. Click to edit the labels of each echelon (Management is same as scale of impact).

## Management of operational risk acceptance thresholds

For information risks:

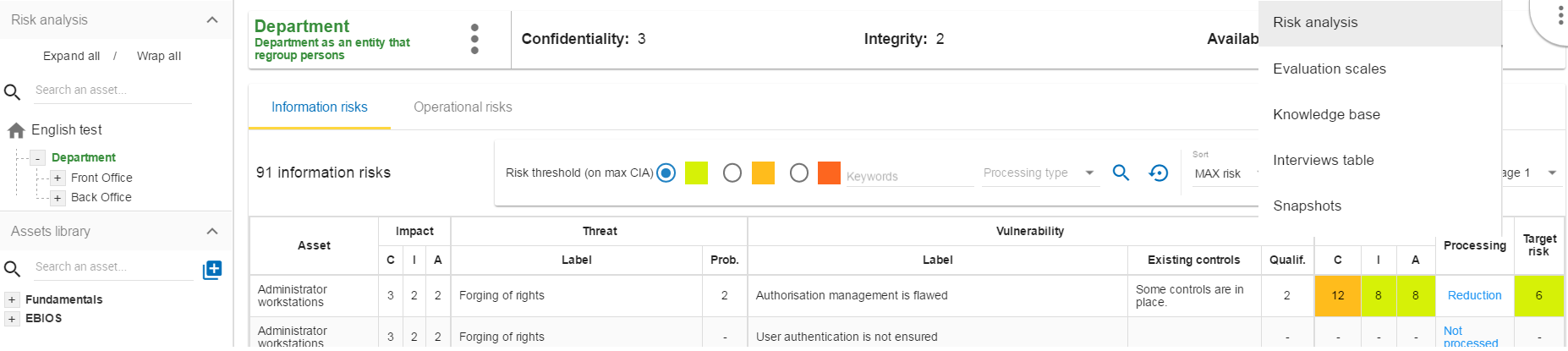
For operational risks:

1. Modification of threshold values. The table just below updates directly, as well as all the risk tables of the analysis.

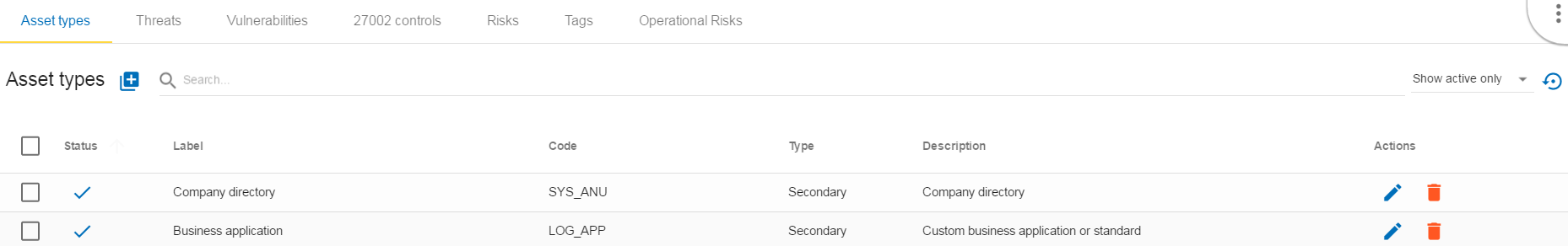
# Management of Knowledge base

 The menu is always accessible from the main view of MONARC:



1. Calling the menu
2. Calling the Management view of evaluation scales

All parameters are managed with the same view:



1. Selecting the desired parameter tab
2. Added a parameter according to the active tab.
3. Finding a parameter.
4. Select a parameter (for deletion).
5. Editing / deleting active parameters.

Generally, all parameters have a code, label, and description

* The code is used to categorize the parameter.
* The label is displayed in all MONARC views.
* The description is the label that typically appears in the tooltip.

## Type of assets

There are two types of assets:

* Primary or business assets: They generally represent, but are not limited to, internal or external services, processes or information. They are the ones that are at the root of the analysis and that will decline their impact on other assets. The containers used to organize the analysis visually are declared as a primary asset (eg Back Office)*.*
* Secondary or supporting assets: These are the assets on which risks are associated, they are used to describe the risk profile of the primary assets.

## Threats

The essential parameters of threat threats are the association with the CIA criteria. It is important when creating a new threat to properly specify these criteria, because they will condition the risk tables.

Example: Passive listening (listening, watching without touching anything) is a threat, for example, that affects only the criterion of confidentiality).

Threats have categories to generate statistics.

## Vulnérabilities

Vulnerabilities must describe the risk context in a negative way. The greater the vulnerability, the less existing or effective measures are. Vulnerability is inverse to maturity.

Example: "Absence of identification of sensitive goods": Low vulnerability if the sensitive goods are identified and vice versa the vulnerability is great if they are not.

The description of the vulnerability is very important because it appears in the risk table as an additional description that helps the security specialist to refine his questionnaire or the precise points that are sought in relation to a risk.

## ISO 27002 controls

It is the repository that is used by default to help the implementation of controls with regard to a specific risk.

## Risks

This table is the core of MONARC's knowledge base. It is here that associations are made between "Asset Type", "Threat" and "Vulnerability". It is the combination of the risks inherent in each asset that will be proposed by default when the risk model is created.

For each association that can be assimilated as a risk scenario, it is possible to associate 1 to 3 security measures from ISO27002 (Guide to good practices in information security).

Only supporting assets are available for a Threat / Vulnerability association.

## Tags (operational risks)

Tags represent a categorization of operational risks. It is a logical grouping of risks that can then be associated with primary assets.

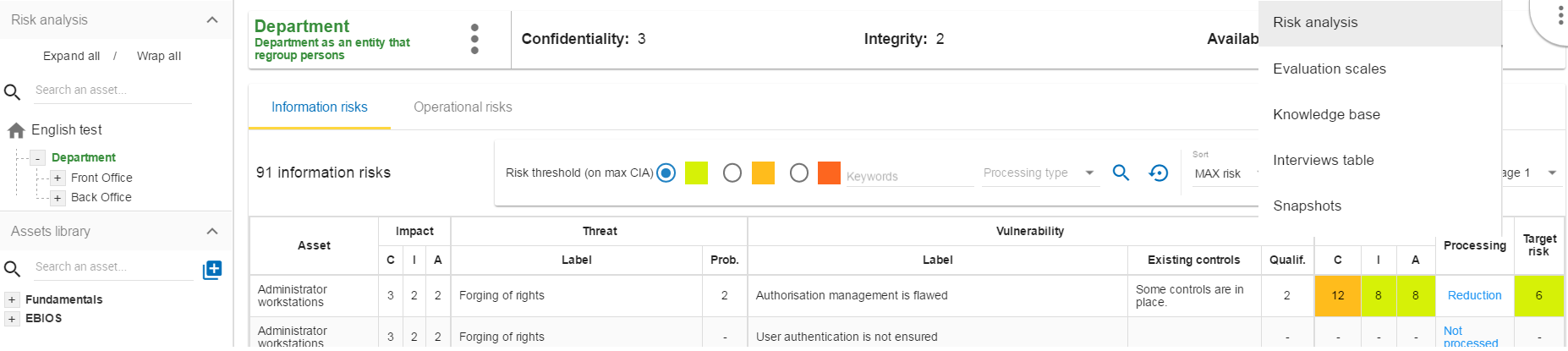
## Operational risks

It is a list of risks created by default or added specifically. Each risk can be associated with one or more tags, which allows, when depositing an asset in the analysis to propose default risks, as for the risks of the information.

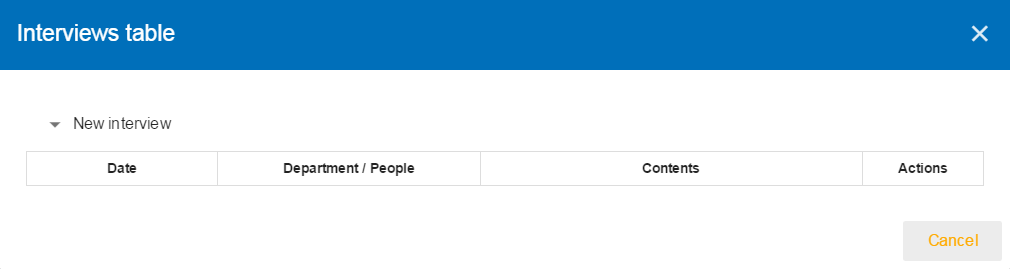
# Gestion des interviews

The interview table allows during a risk analysis to list in the final report, the various interviews that were necessary to collect the information. Information such as dates, interviewees can be entered for a comprehensive report.

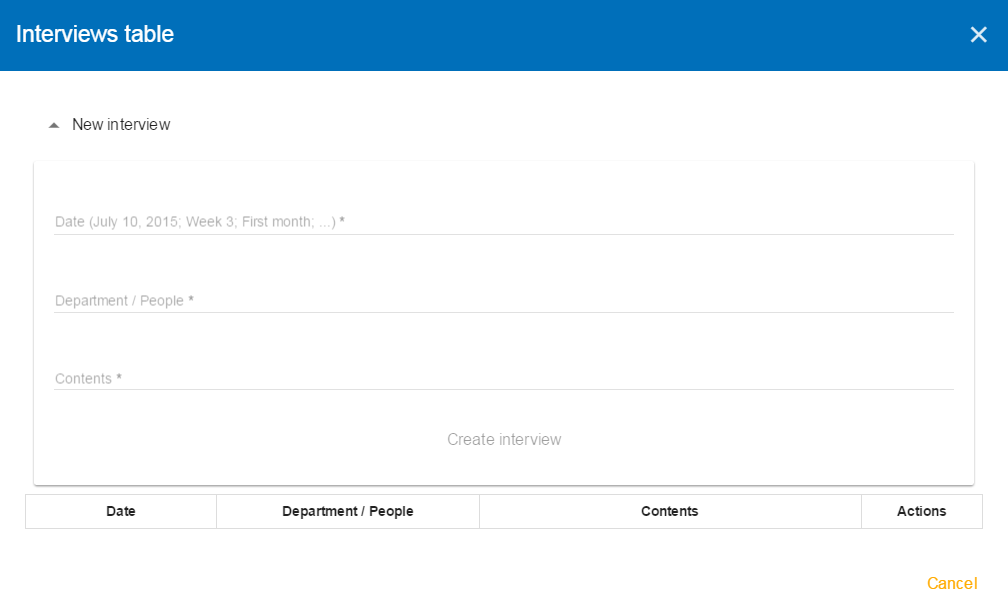
 The menu is always accessible from the main view of MONARC:



1. Calling the menu
2. Calling the Management view of evaluation scales

1. Click to encode a new interview

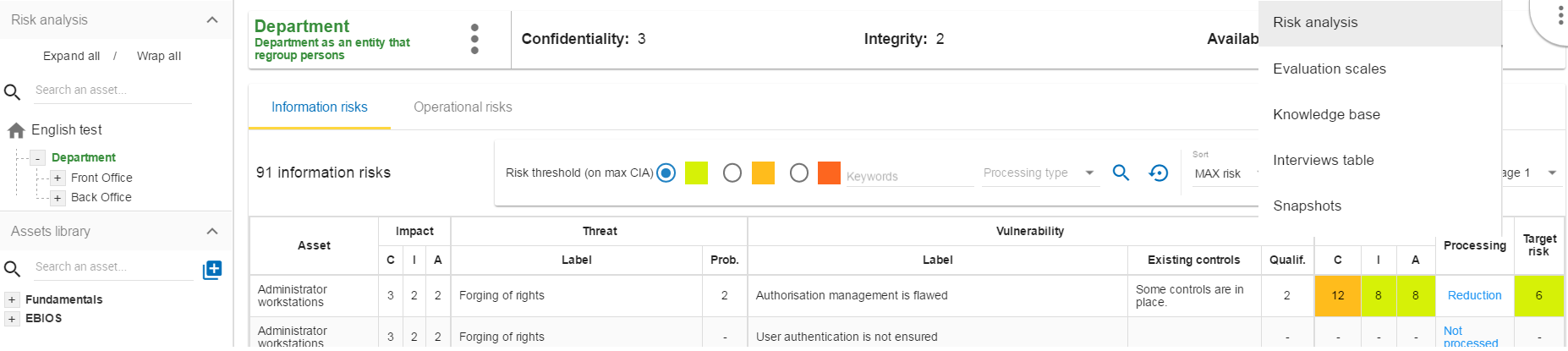
 

1. Information to be entered: date, names of persons and possibly subjects covered.

# Snapshots

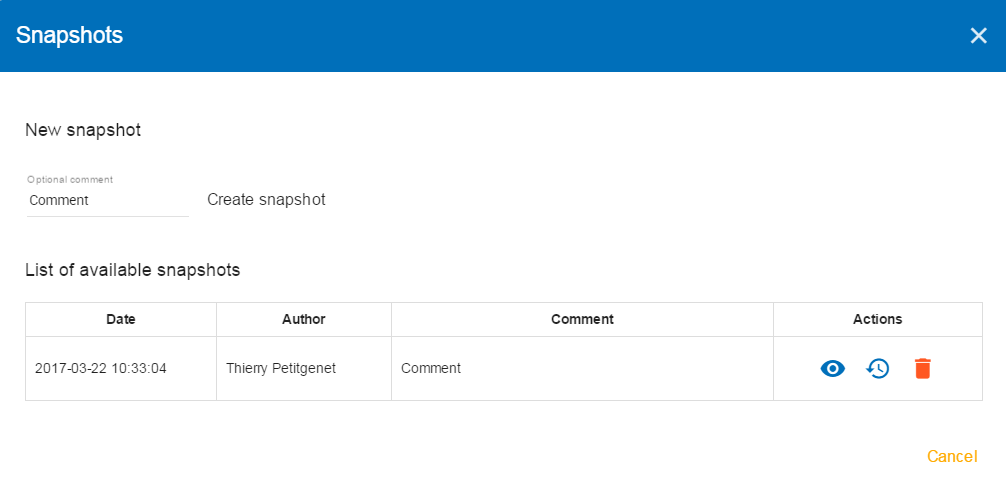
Snapshots allow you to create a full backup of an analysis. *It is a function to use regularly during the course, before and after great changes, because it is the only way to go back in the changes.*

 The menu is always accessible from the main view of MONARC:



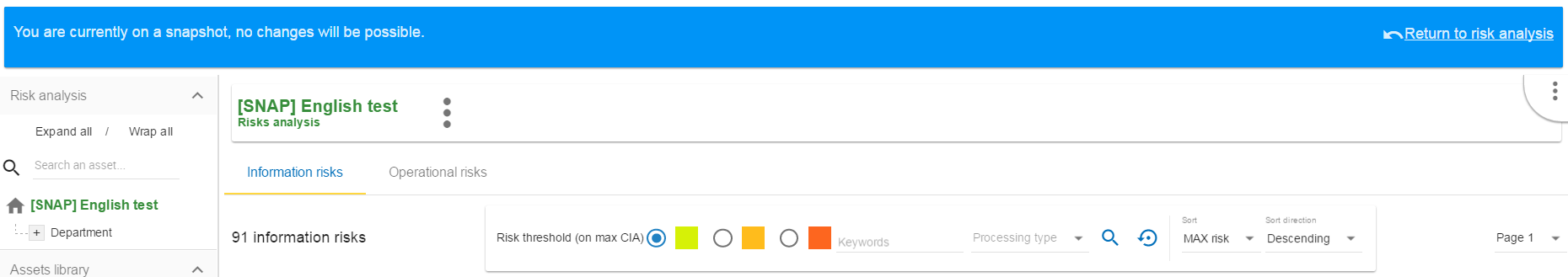
1. Calling the menu
2. Calling the Management view of evaluation scales

The following pop-up appears:

1. Creating a Snapshot: Possibility to enter a comment allowing to contextualize the Snapshot.
2. Possible actions:
   1. View a Snapshot
   2. Restore Snapshot. Caution this option will overwrite the current analysis.
   3. Delete a Snapshot.

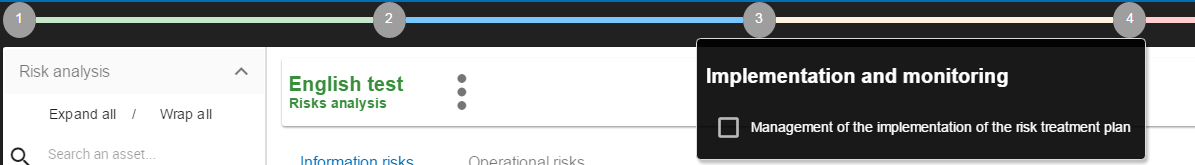
When viewing a Snapshot, no changes are possible, and the blue bar as shown above is displayed:

1. Click on the button to return to normal operation.

# Managing the implementation treatment plan

By clicking on the number 4 on the method bar, the following menu appears:



This view goes beyond the ISO / IEC 27005 standard, because it allows to manage the follow-up of the implementation of the conntrols.

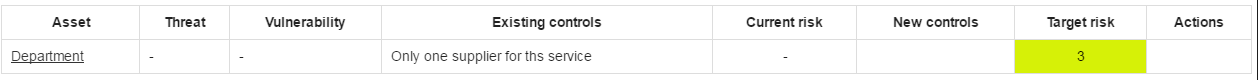
The current version is in Beta, it is developed but waiting for users to return for improvement.

By clicking on the link "Managing the Implementation of the Risk Management Plan", the following view appears, listing all the recommendations made by the analysis.

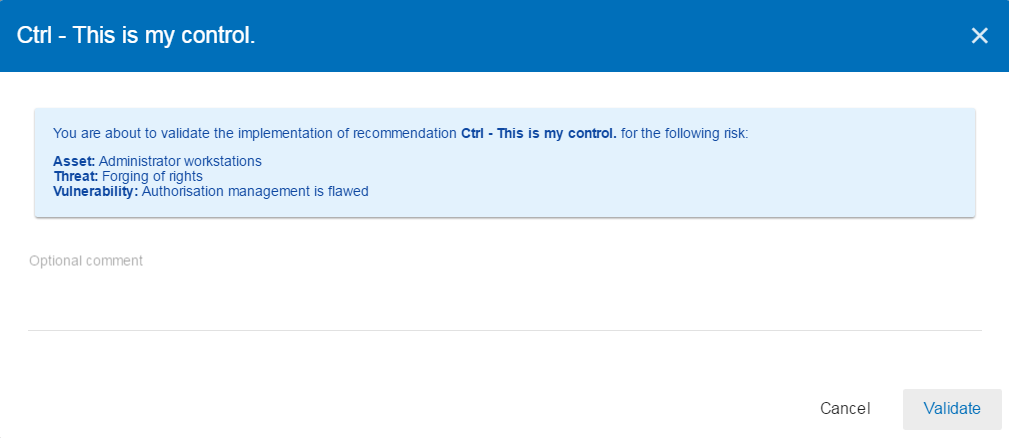


1. Name of the recommendation
2. Comment on recommendation
3. Responsible for the implementation of the recommendation
4. Deadline for the implementation of the recommendation
5. Status of Implementation
6. When the recommendation has been implemented, click on action will start the process of updating the risks (continued below)

This view lists all the risks that are dependent on the recommendation. Then, for each risk, the following information is entered:



1. Various information concerning the risk
2. Encode the new finding, as is the case after updating the recommendation
3. Launches the pop-up validation of the update below



After validation, the risk concerned becomes the current risk, the recommendation is deleted from the risk concerned.

All validations are stored in a history and can be consulted:



1. Click to view past recommendations

