MONARC User guide

"security made in Lëtzebuerg" (SMILE) g.i.e.

Table of Contents

1. Introduction

1.1. Purpose

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

1.2. Other documents

- **Quick Start**: Provide a quick start with MONARC.
- **Method guide**: Complete documentation of the method.
- **Technical guide**: Complete technical documentation.

1.3. Syntax used in the document

❶

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.).

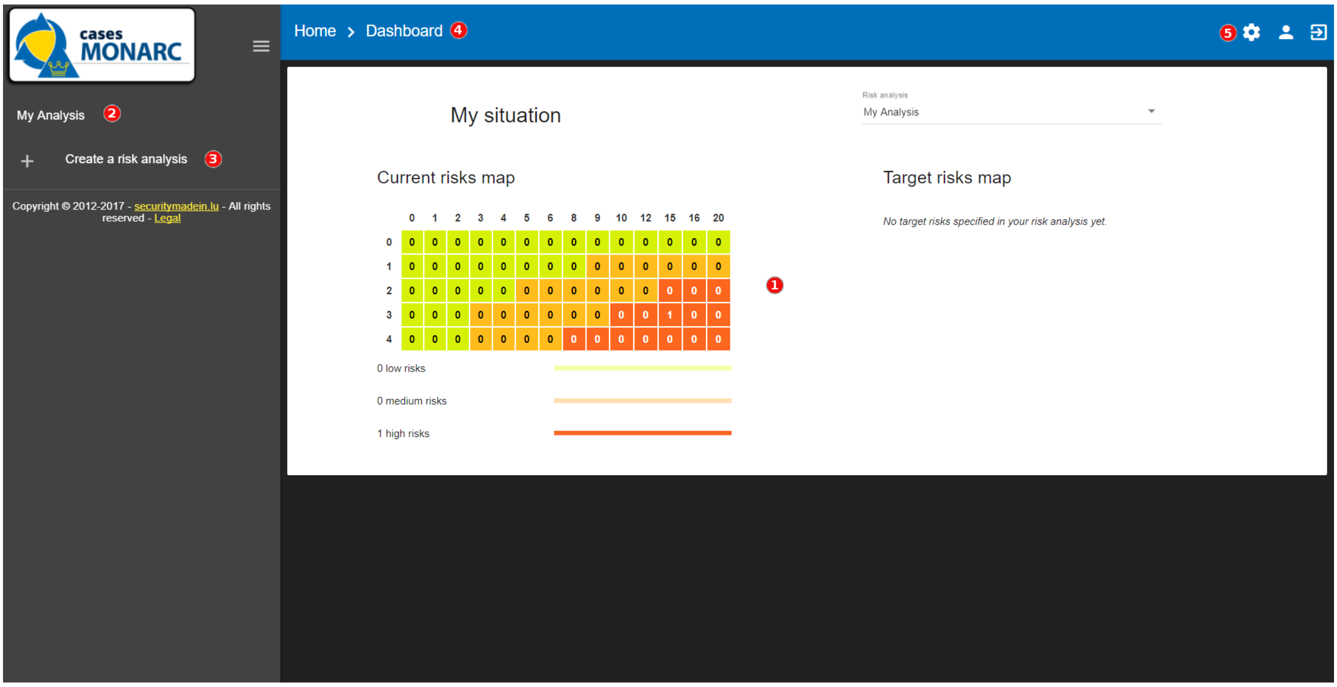
☝

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

2. Home Page

2.1. 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.



Copyright © 2012-2017 - securitymadein.lu - All rights reserved - Legal

My situation

Current risks map

	0	1	2	3	4	5	6	8	9	10	12	15	16	20
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	1	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0

0 low risks

0 medium risks

1 high risks

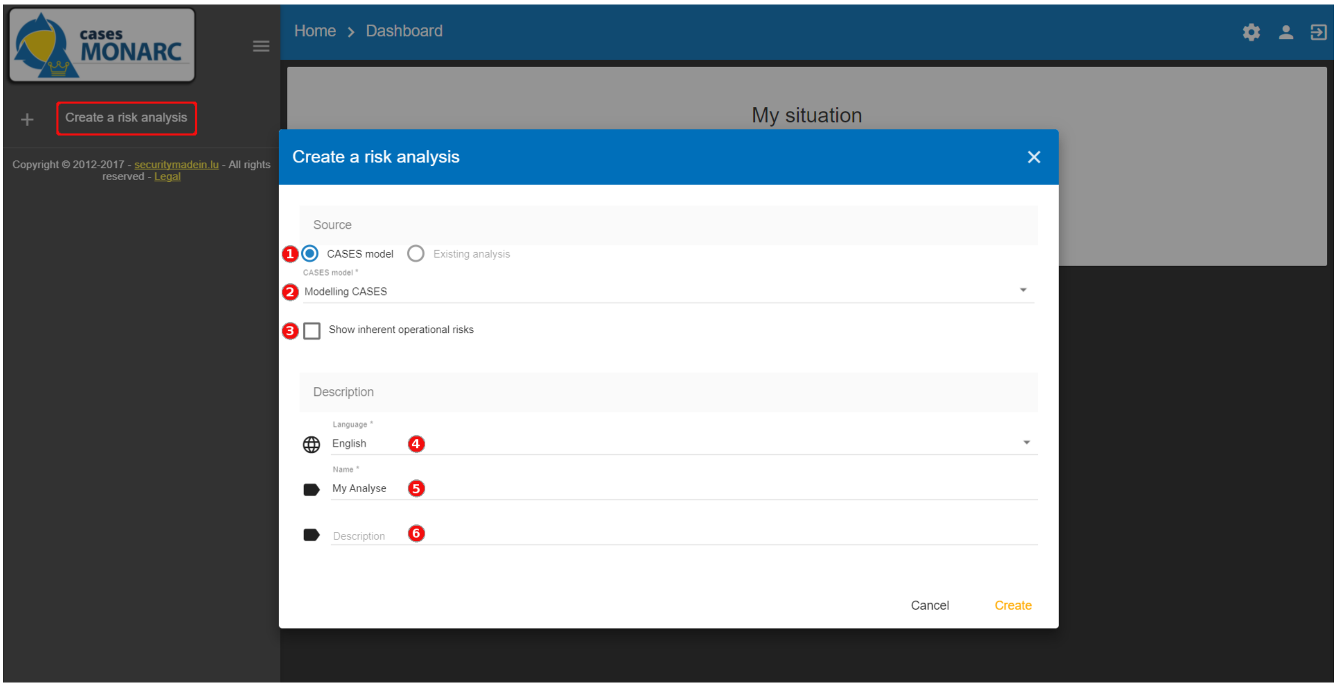
Target risks map

No target risks specified in your risk analysis yet.

1. Graph showing the statistics of the last modified risk analysis.
2. List of existing analyzes. In this case, there is only one. Click on the analysis to select it. (see Main risk analysis view)
3. Click to `create a risk analysis` (see Creating a Risk Analysis).
4. Navigation bar
5. Administration of the client environment. Click on `Manage users`, `Account` or `Logout` (see Client Environment Administration).

2.2. Creating a Risk Analysis

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



Source

● CASES model ○ Existing analysis

CASES model *: Modelling CASES

□ Show inherent operational risks

Description

Language *: English

Name *: My Analyse

Description

1. The creation of a risk analysis is always based on an existing model. There are two choices for this:

   a. `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 a risk analysis. This option should be used by default to start a new risk 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 file, for example.

   b. `Existing analysis`: Duplicate a risk analysis of your choice present in your environment.

2. Options ***a*** or ***b*** before selected. It get the source.

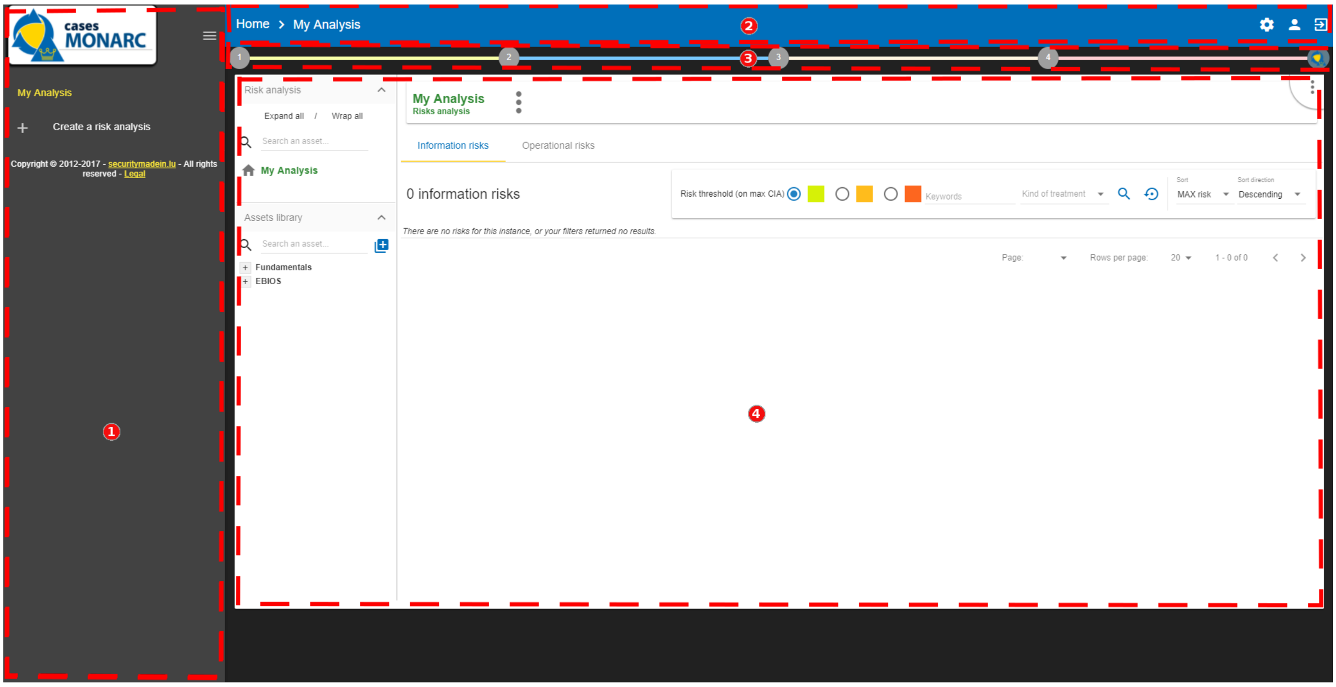
3. `Show inherent operational risks`. (see Operational risks)

4. Select the preferred language for this new risk analysis. MONARC only present the languages actually available in the selected source.

5. Give your risk analysis a name.

6. Optional field, which allows you to describe your analysis in more detail.

2.3. Main risk analysis view



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

1. Risk Analyses panel: Create and select a risk analysis.

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

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

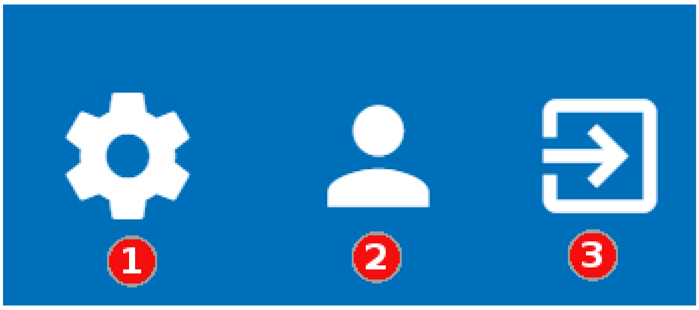
3. Client Environment Administration

There are two profiles:

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

By risk analysis, there are 3 types of rights:

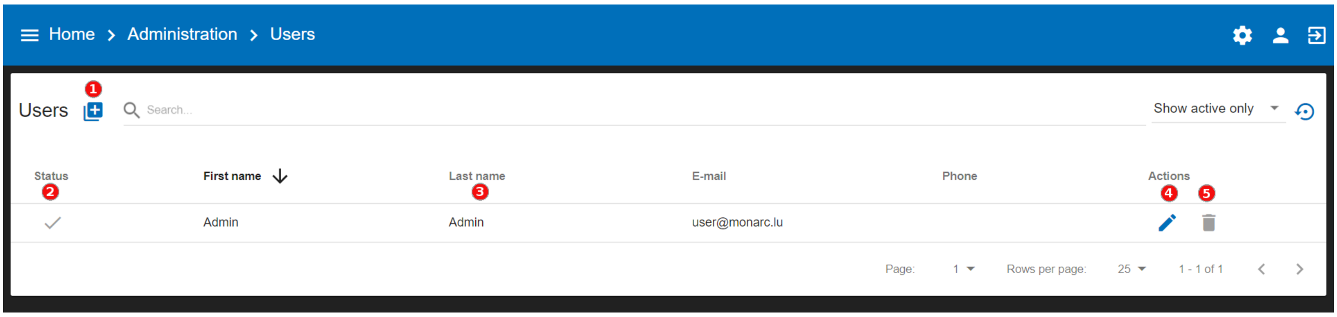
- No access.
- Read only.
- Read and write.



1. Administration (Enable only for administrator user)
2. User account
3. Logout

3.1. Administration of users

3.1.1. List of users



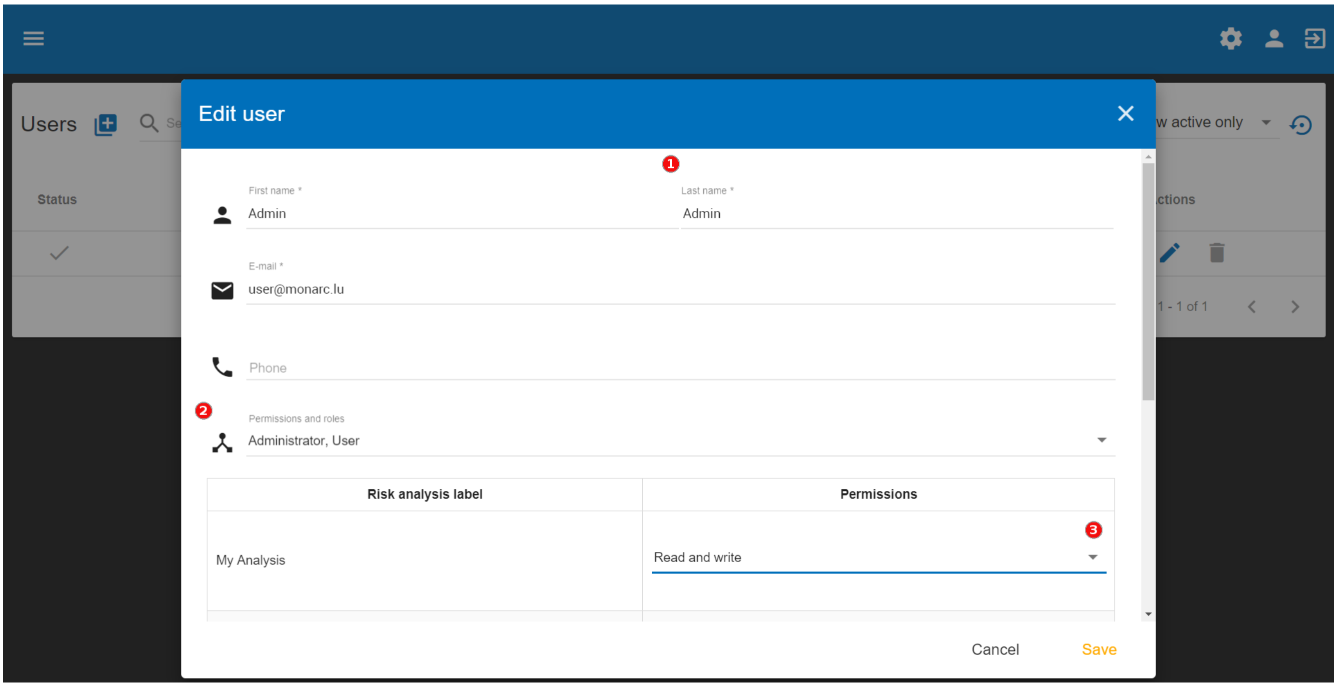
Status	First name	Last name	E-mail	Phone	Actions
✓	Admin	Admin	user@monarc.lu		✏ 🗑

Page: 1 Rows per page: 25 1 - 1 of 1

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.

3.1.2. User rights and information

After clicking the ✏ icon, the following screen appears:



First name * Admin

Last name * Admin

E-mail * user@monarc.lu

Phone

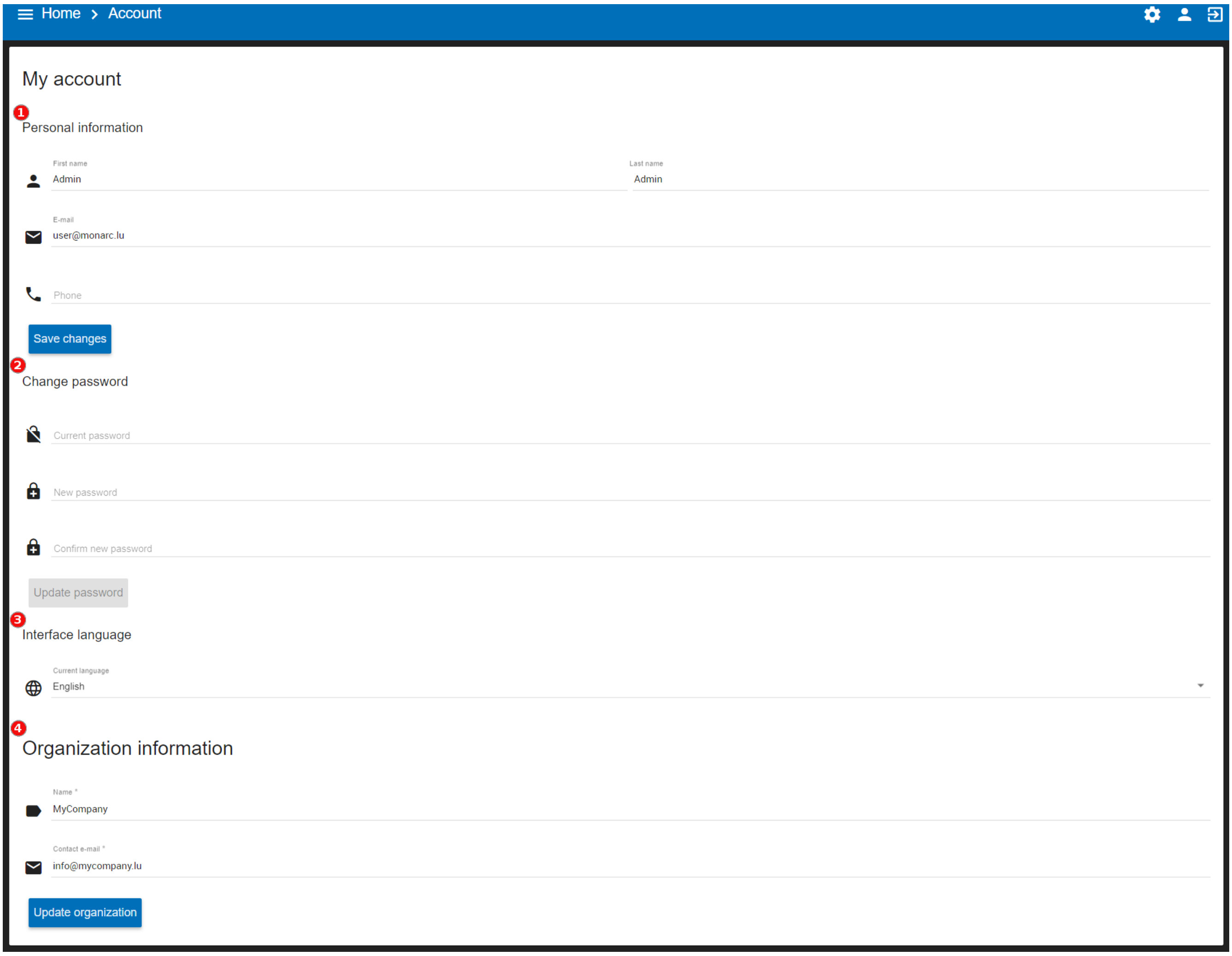
Permissions and roles: Administrator, User

Risk analysis label	Permissions
My Analysis	Read and write

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

3.2. User account

This view allows you to:



My account

Personal information

First name: Admin

Last name: Admin

E-mail: user@monarc.lu

Phone

Change password

Current password

New password

Confirm new password

Interface language

Current language: English

Organization information

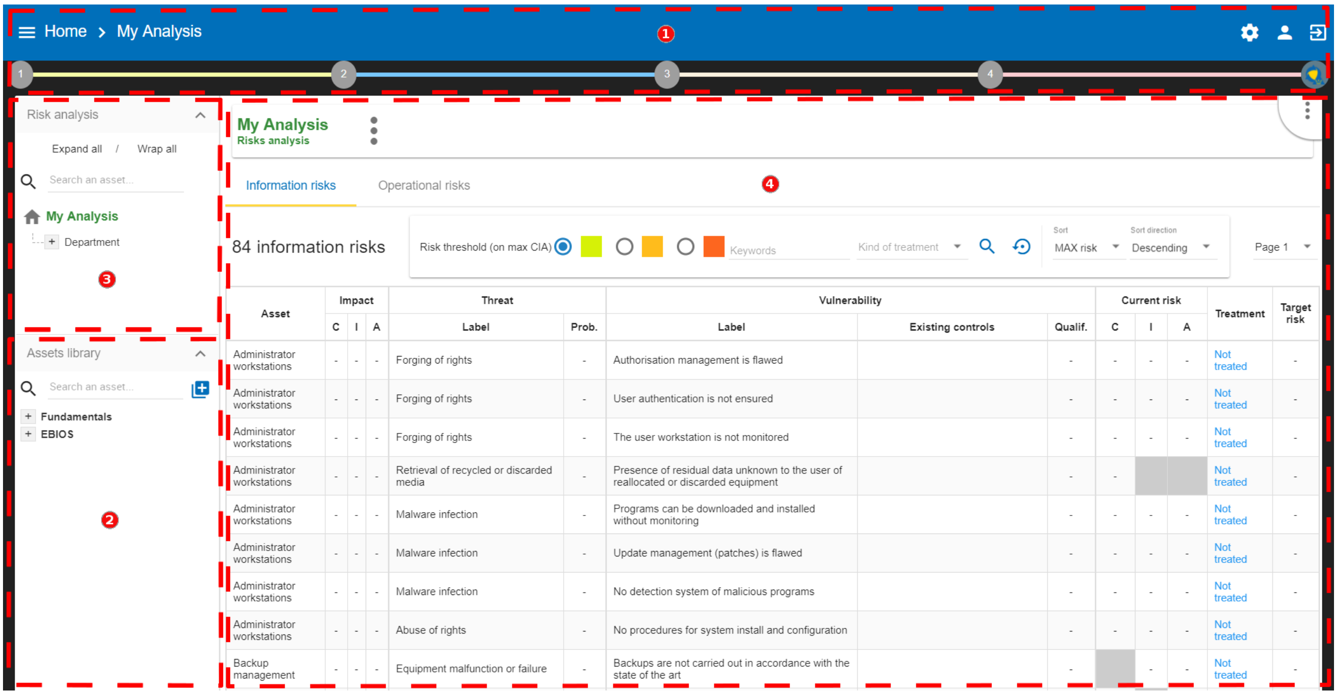
Name *: MyCompany

Contact e-mail *: info@mycompany.lu

1. Manage general user information.
2. Change the password. Password complexity is required.
3. 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)
4. Manage general information about the entity (MONARC account).

4. Analysis management

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



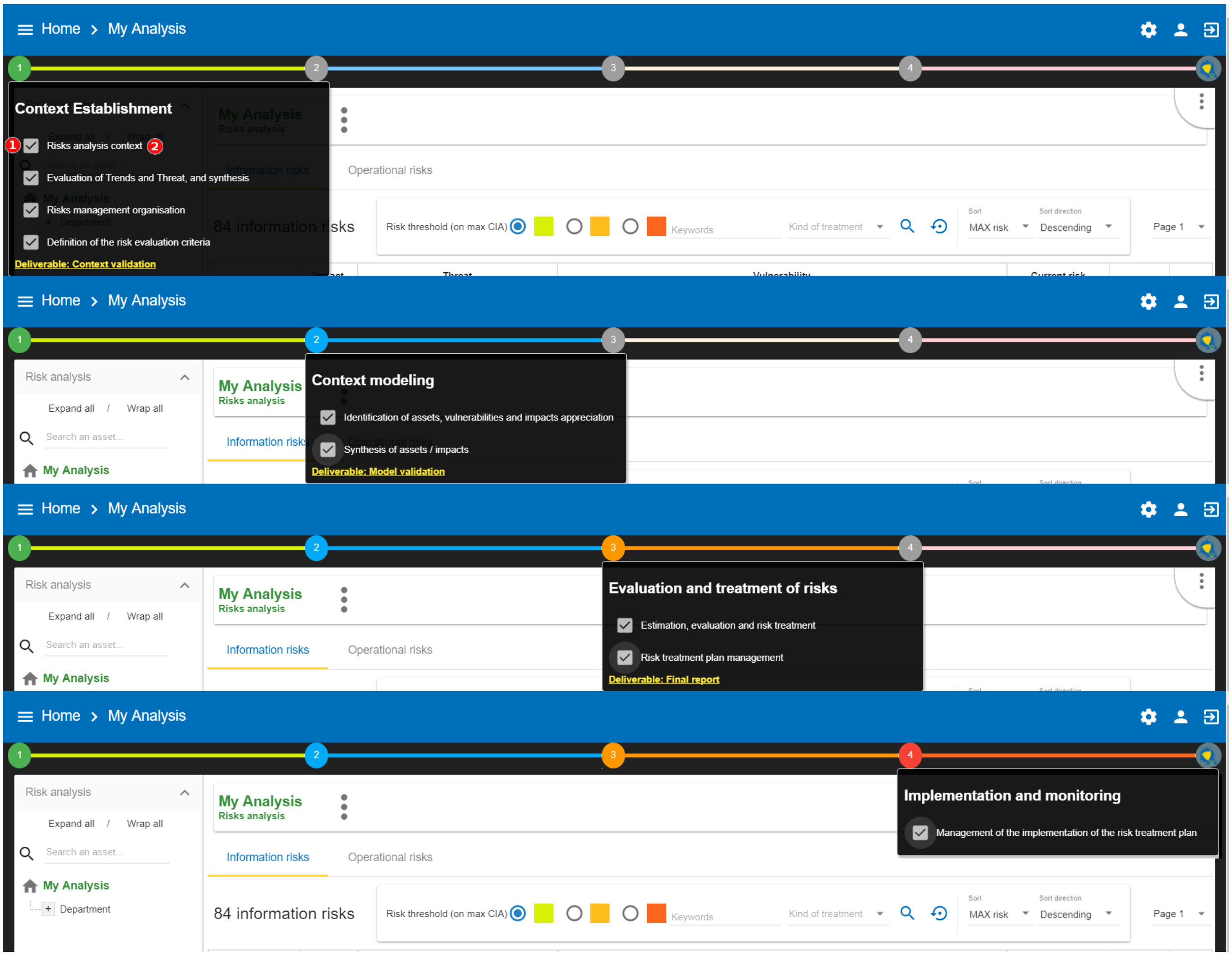
84 information risks

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Target risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-			Not treated	-
Administrator workstations	-	-	-	Malware infection	-	Programs can be downloaded and installed without monitoring		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Malware infection	-	Update management (patches) is flawed		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Malware infection	-	No detection system of malicious programs		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Abuse of rights	-	No procedures for system install and configuration		-	-	-	-	Not treated	-
Backup management	-	-	-	Equipment malfunction or failure	-	Backups are not carried out in accordance with the state of the art		-		-	-	Not treated	-

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 Method steps calls).
2. Asset library area: Asset storage. The *drag-and-drop* function must be used to place these assets in the analysis (see Library).
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). (See Information Risks and Operational Risks)
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.

4.1. Method steps calls

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



Context Establishment

1 ☑ Risks analysis context 2

☑ Evaluation of Trends and Threat, and synthesis

☑ Risks management organisation

☑ Definition of the risk evaluation criteria

Deliverable: Context validation

Context modeling

☑ Identification of assets, vulnerabilities and impacts appreciation

☑ Synthesis of assets / impacts

Deliverable: Model validation

Evaluation and treatment of risks

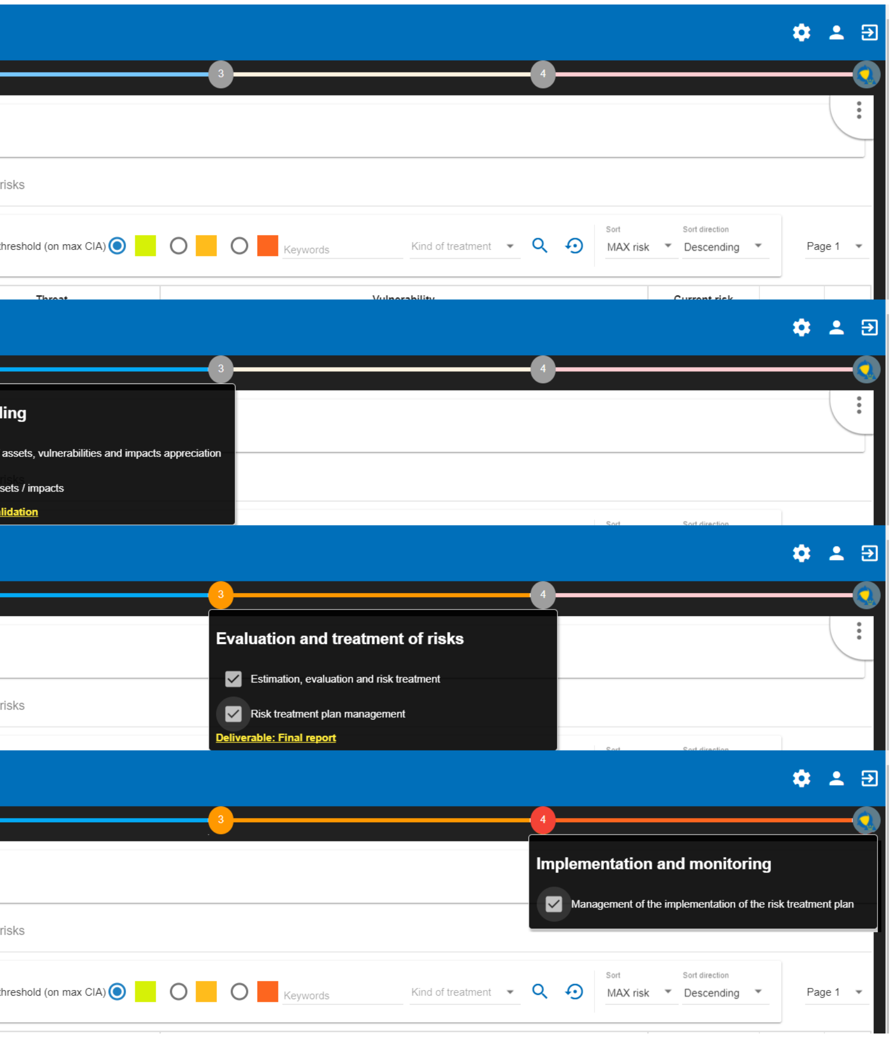
☑ Estimation, evaluation and risk treatment

☑ Risk treatment plan management

Deliverable: Final report

Implementation and monitoring

☑ Management of the implementation of the risk treatment plan



ling

assets, vulnerabilities and impacts appreciation

sets / impacts

lidation

Evaluation and treatment of risks

☑ Estimation, evaluation and risk treatment

☑ Risk treatment plan management

Deliverable: Final report

Implementation and monitoring

☑ Management of the implementation of the risk treatment plan

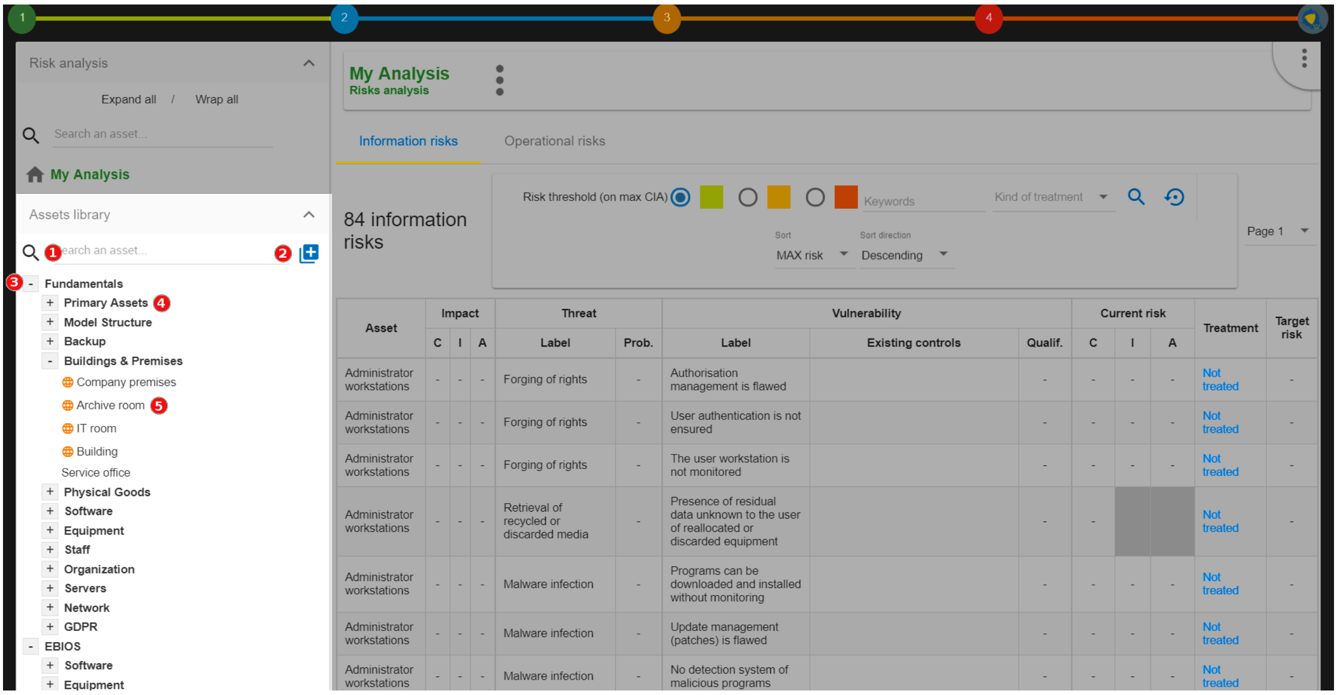
1. Ticking the boxes change the progress of the method.
2. Click on the label, call the contextual management sub-screen.

More information about method steps. Consult the **method guide**.

4.2. Library

4.2.1. Organization of assets

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



84 information risks

Sort: MAX risk

Sort direction: Descending

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Target risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-			Not treated	-
Administrator workstations	-	-	-	Malware infection	-	Programs can be downloaded and installed without monitoring		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Malware infection	-	Update management (patches) is flawed		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Malware infection	-	No detection system of malicious programs		-	-	-	-	Not treated	-

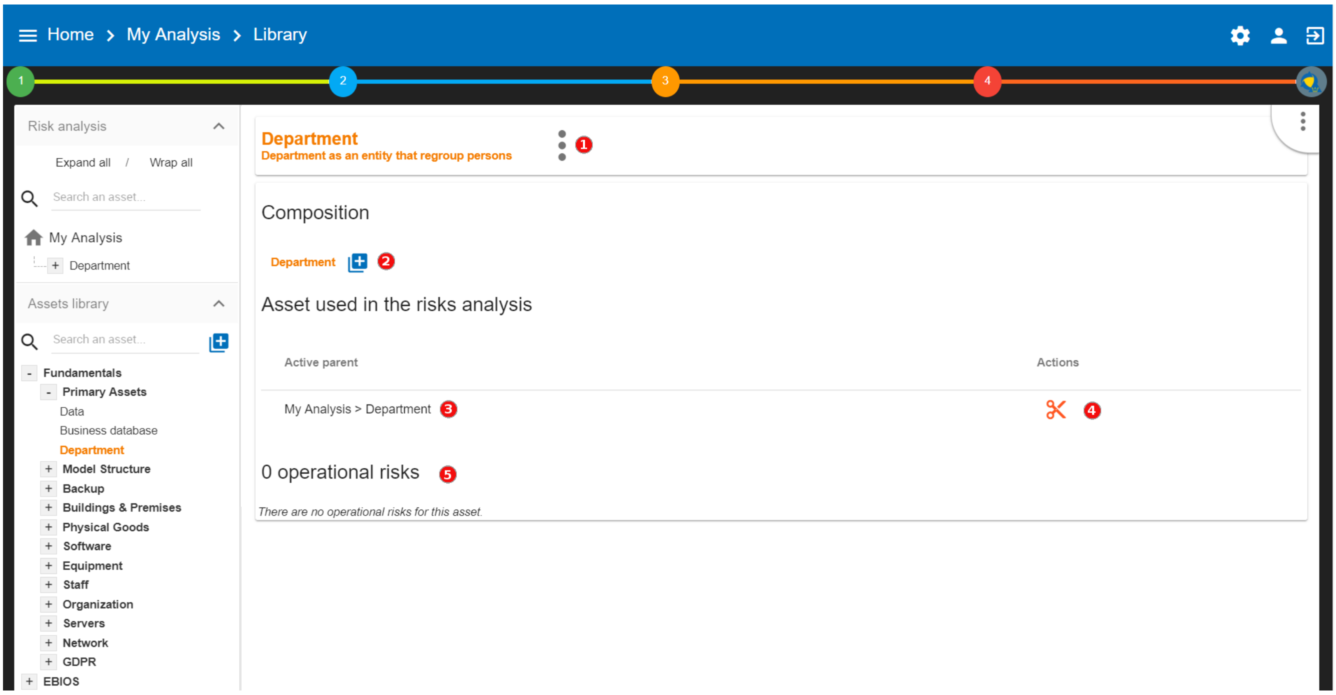
1. Search area in order to quickly find an asset.
2. Button for creating / importing assets (see Create an Asset).
3. Categories level of the library. There are usually two:
    a. Fundamentals: Contains all default assets offered by CASES.
    b. EBIOS: Contains assets inspired by EBIOS. These are assets containing non-optimized risk models.
4. Sub-categories level.
5. Asset level: These are the assets that must be dragging and dropping in the risk analysis area.

4.2.2. Asset Management

The information on each asset is different depending on its type: Primary or Secondary. This concept is explained in detail in Type of assets.

Primary asset

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



Department as an entity that regroup persons

Active parent	Actions
My Analysis > Department	

There are no operational risks for this asset.

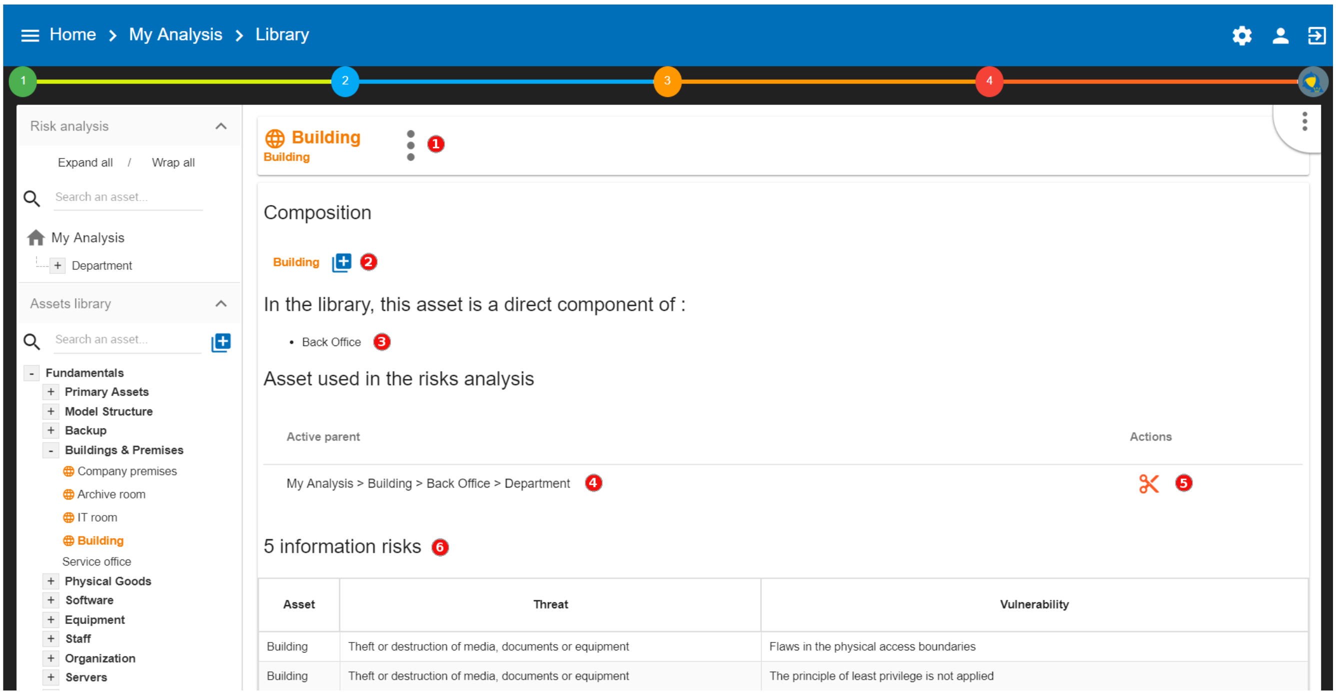
1. Asset management context menu (details in [Context menu]).
2. Add an existing asset in the structure, creating a composed asset. There is no limit in the asset tree.
3. Indication if this asset is currently used in the analysis. In this case, it is found at the root of the analysis.
4. Ability to detach asset from analysis.
5. Table of operational risks possibly associated with the asset.

Detach an asset from the analysis will remove all its evaluation.

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 `Fundamentals` → `Buildings & Premises`.



Home > My Analysis > Library

1 2 3 4

Risk analysis

Expand all / Wrap all

Search an asset...

My Analysis

- Department

Assets library

Search an asset...

- Fundamentals
  - Primary Assets
  - Model Structure
  - Backup
  - Buildings & Premises
    - Company premises
    - Archive room
    - IT room
    - Building
    - Service office
  - Physical Goods
  - Software
  - Equipment
  - Staff
  - Organization
  - Servers

Building
Building 1

Composition

Building 2

In the library, this asset is a direct component of :

- Back Office 3

Asset used in the risks analysis

Active parent	Actions
My Analysis > Building > Back Office > Department 4	5

5 information risks 6

Asset	Threat	Vulnerability
Building	Theft or destruction of media, documents or equipment	Flaws in the physical access boundaries
Building	Theft or destruction of media, documents or equipment	The principle of least privilege is not applied

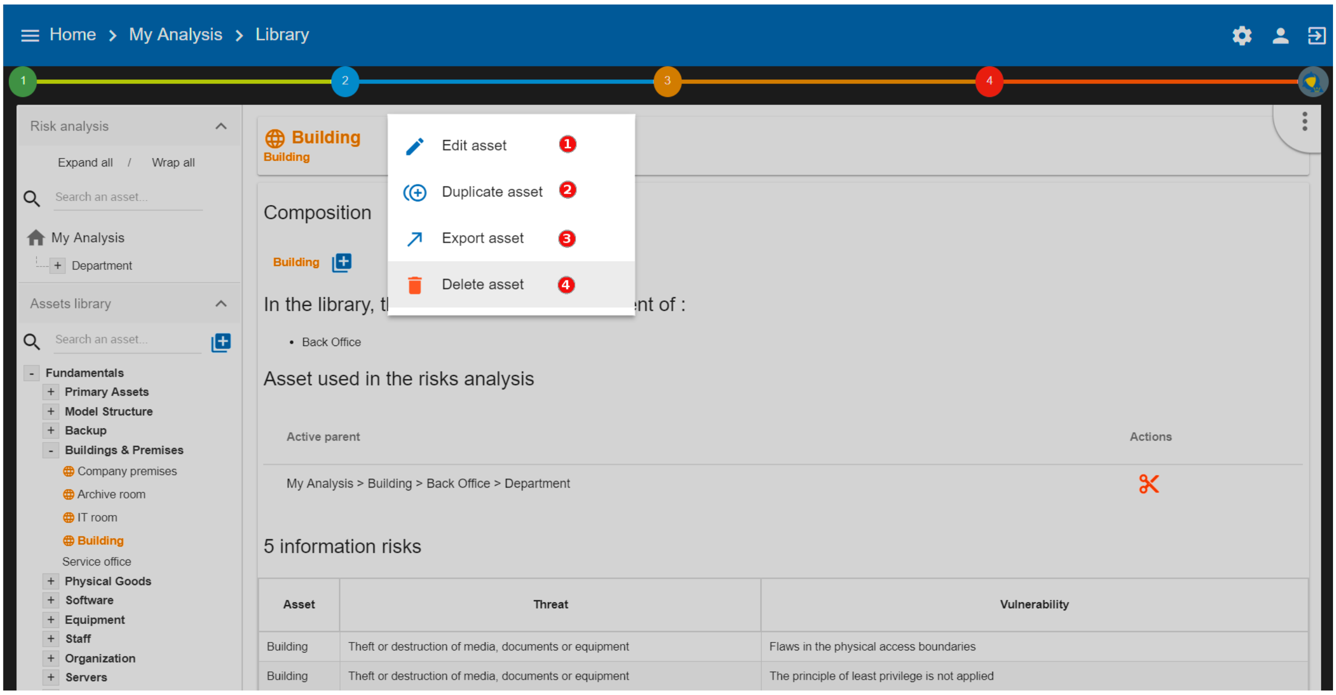
1. Asset management context menu (details in [Context menu]).
2. Add an existing asset in the structure, creating a compound asset. There is no limit in the asset tree.
3. Indication if the asset is already part of the composition of another asset. In case, it is already a sub-element of the assets `Back 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 risk analysis.
5. Ability to detach asset from analysis.
6. Risk information table associated with the asset.

Detach an asset from the analysis will remove all its evaluation.

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 of library

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



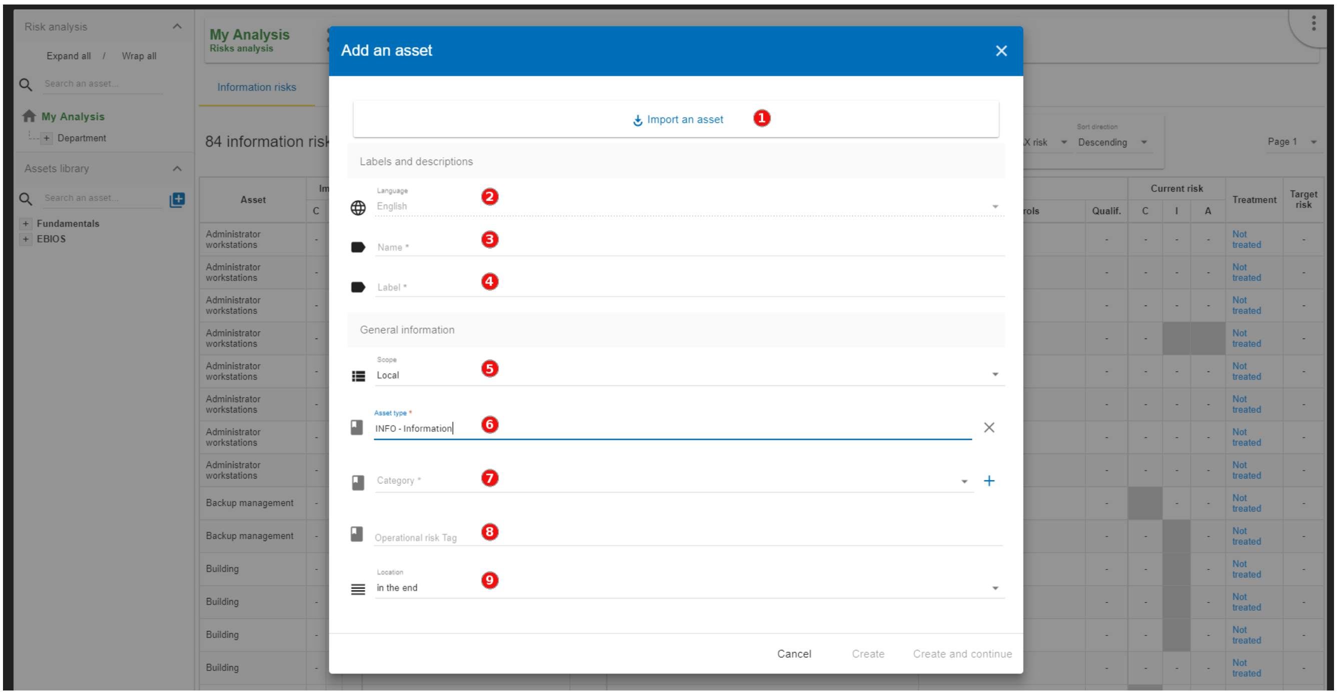
Asset	Threat	Vulnerability
Building	Theft or destruction of media, documents or equipment	Flaws in the physical access boundaries
Building	Theft or destruction of media, documents or equipment	The principle of least privilege is not applied

1. Starts the pop-up that allows you to modify most of the parameters of an asset (see Edit an asset).
2. Create a copy of the asset named `Name (copy # 1)`, which is then renamed with the `Edit Asset` option.
3. Launches asset export pop-up (see Exporting an asset).
4. Delete an asset.

Delete action is definitive, even if the asset is used in the analysis.

4.2.3. Create an Asset

In the library, after clicking on ⊞ , the following pop-up appears:



Add an asset

Import an asset 1

Labels and descriptions

Language: English 2

Name * 3

Label * 4

General information

Scope: Local 5

Asset type *: INFO - Information 6

Category * 7

Operational risk Tag 8

Location: in the end 9

1. To create an asset, it is also possible to import it (see Importing an asset).
2. `Language`: This option cannot be used, the default language of the analysis is imposed.
3. `Name`: This name must be unique for the analysis.
4. `Label`: This is an additional description, it is displayed in the tooltip when the mouse is positioned without moving on the asset.
5. `Scope`: Two possible choices:
    a. `Local`: Identified asset risks are to be assessed whenever the asset is present in the analysis. A primary asset is generally local in scope.
    b. `Global` 🌐 : The 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**: For IT room or main building, once the risks assessed, only the impact from the primary asset can change the level of risk.

6. `Asset type`: It determines the nature of the asset and therefore the risk model associated with it.
7. `Category`: It is the location in the library where the asset will be stored, or create a new category.
8. `Operational risk Tag`: , that allows the asset to be associated with operational risks by default.

> This option is enable only when asset type is a primary (**i.e**. Information, process, container or service)

9. `Location`: Allows you to order assets in the selected category.

4.2.4. Edit an asset

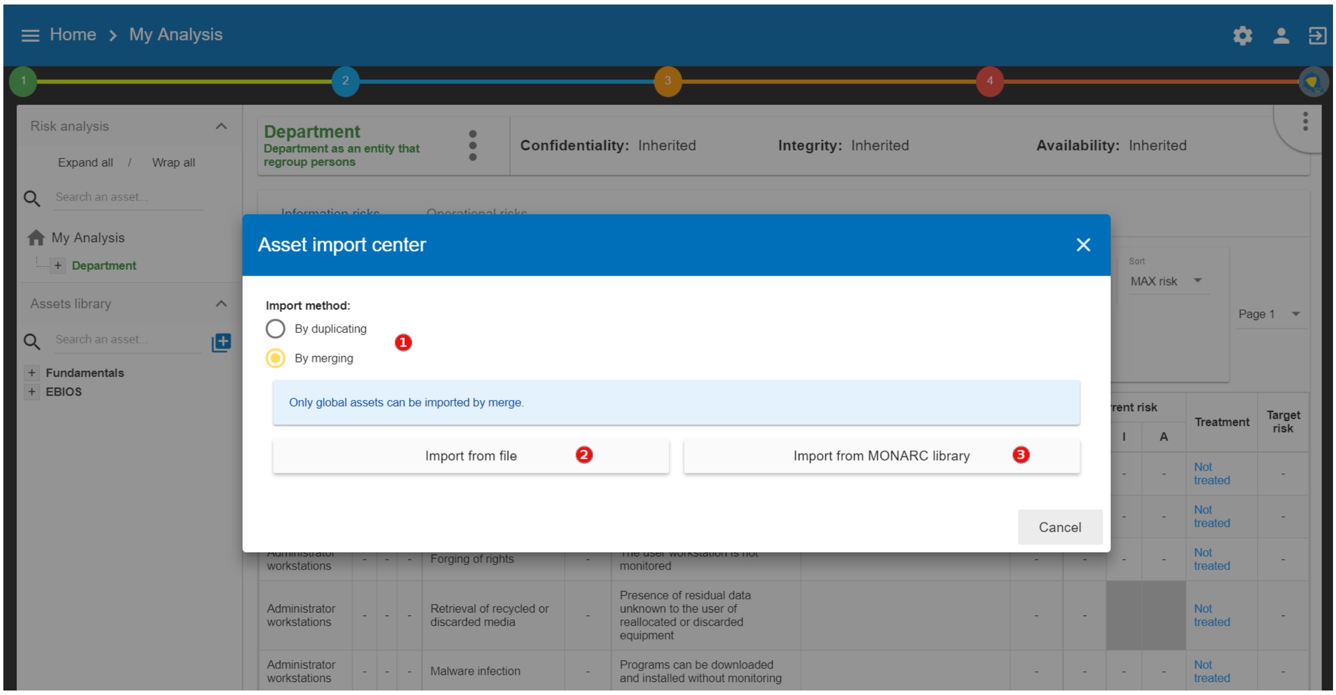
The call is made from the context menu when an asset is selected in the library.

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

- `Language`
- `Scope`
- `Asset type`

4.2.5. Importing an asset

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


Asset import center

Import method:

○ By duplicating (1)

● By merging

Only global assets can be imported by merge.

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

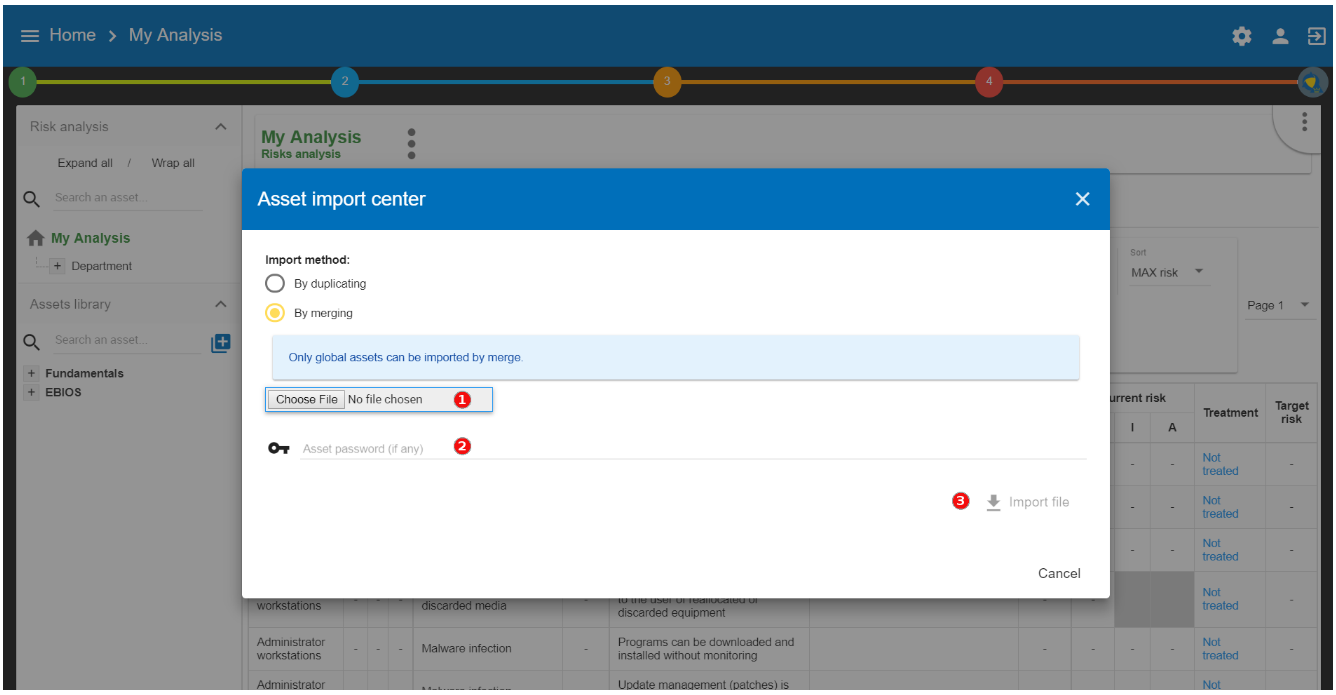
    Only global assets can be imported by merge.

2. `Import from file`: allows to exchange assets from one environment to another (see Importing an asset from a file).
3. `Import from MONARC library`: This option is not available in the case of a *Stand alone* version of MONARC (see Import from the MONARC library).

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

Importing an asset from a file

The pop-up appears after clicking on the `Import from file` option in the `Asset Import center`.



Asset import center

Import method:

○ By duplicating

● By merging

Only global assets can be imported by merge.

Choose File No file chosen ❶

Asset password (if any) ❷

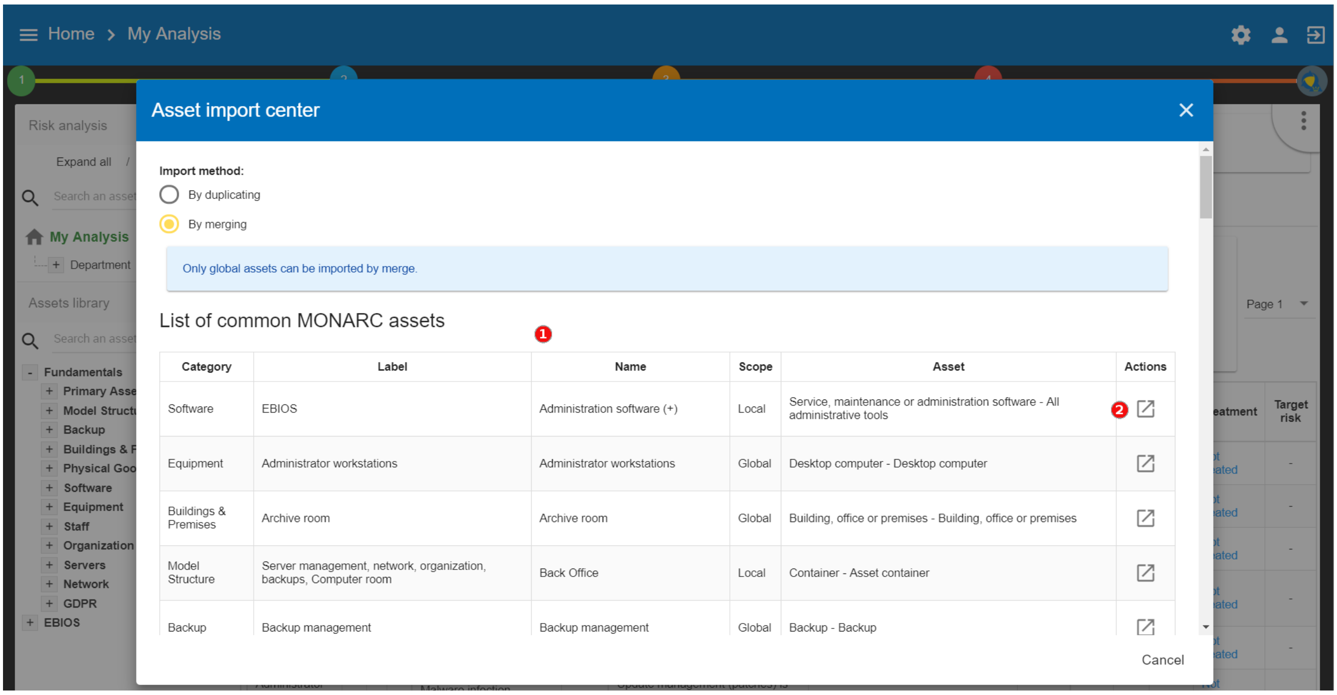
❸ Import file

Cancel

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

Import from the MONARC library

The pop-up appears after clicking on the `Import from MONARC library` option in the `Asset Import center`.



Asset import center

Import method:

○ By duplicating

● By merging

Only global assets can be imported by merge.

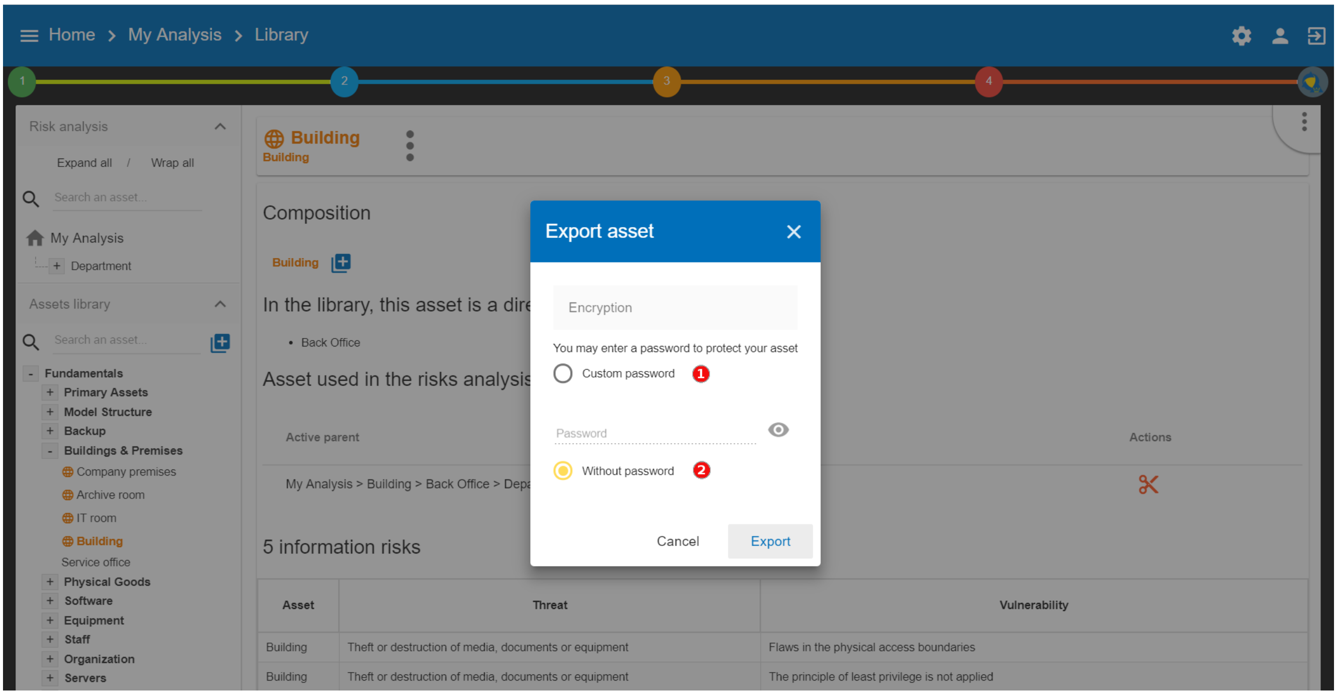
List of common MONARC assets ❶

Category	Label	Name	Scope	Asset	Actions
Software	EBIOS	Administration software (+)	Local	Service, maintenance or administration software - All administrative tools	❷ ↗
Equipment	Administrator workstations	Administrator workstations	Global	Desktop computer - Desktop computer	↗
Buildings & Premises	Archive room	Archive room	Global	Building, office or premises - Building, office or premises	↗
Model Structure	Server management, network, organization, backups, Computer room	Back Office	Local	Container - Asset container	↗
Backup	Backup management	Backup management	Global	Backup - Backup	↗

Cancel

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

4.2.6. Exporting an asset



Export asset

Encryption

You may enter a password to protect your asset

○ Custom password 1

Password

● Without password 2

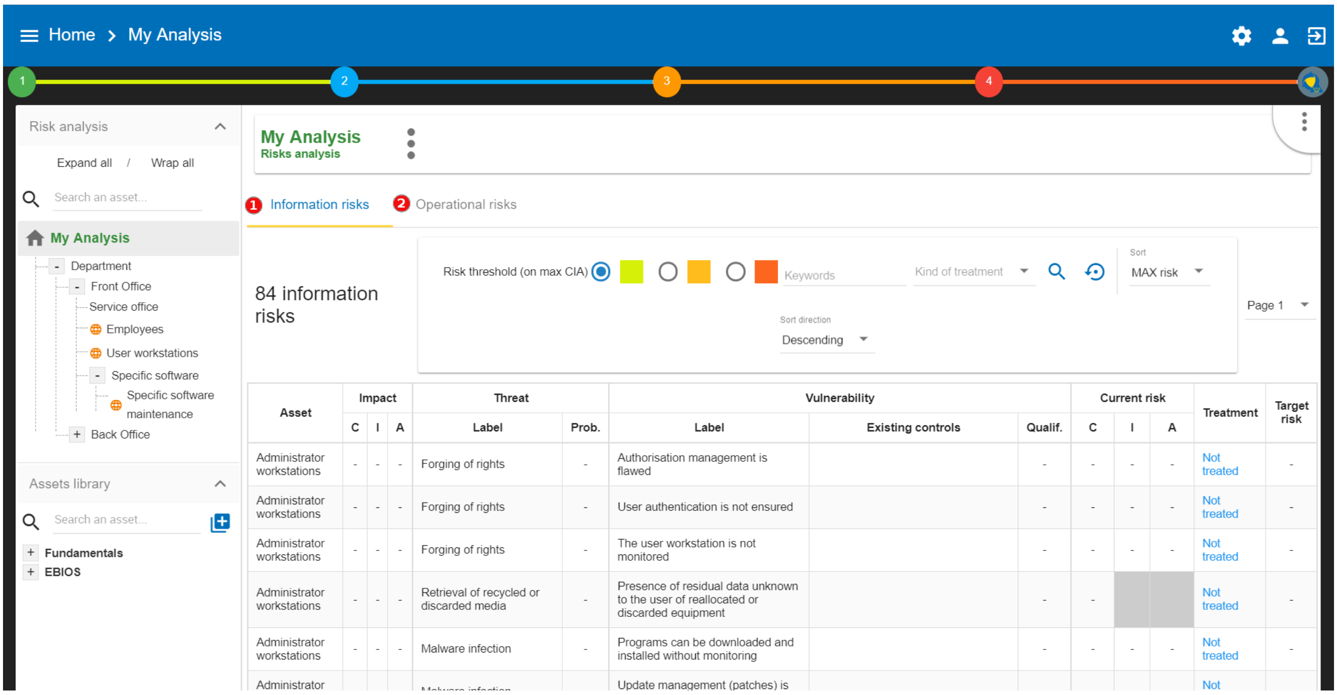
Asset	Threat	Vulnerability
Building	Theft or destruction of media, documents or equipment	Flaws in the physical access boundaries
Building	Theft or destruction of media, documents or equipment	The principle of least privilege is not applied

1. `Custom password`: Possibility to encrypt the generated file with a symmetric password that will be necessary during the import.
2. `Without password`: Default password sets by tool.

> This option ensures only the file integrity.

4.3. Information Risks

By selecting the top of the analysis or an asset in the tree, the risk table appears. There are two separate risk tables:



84 information risks

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

Sort: MAX risk

Sort direction: Descending

Page 1

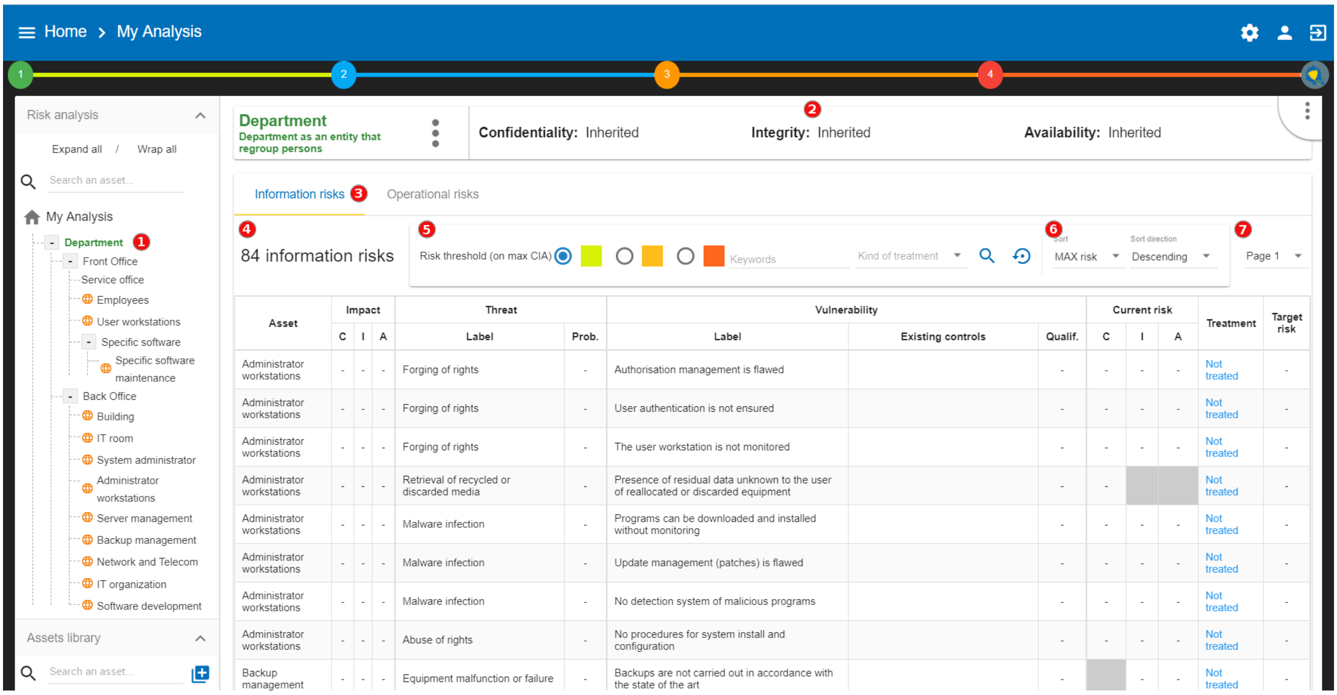
Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Target risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-			Not treated	-
Administrator workstations	-	-	-	Malware infection	-	Programs can be downloaded and installed without monitoring		-	-	-	-	Not treated	-
Administrator				Malware infection		Update management (patches) is						Not	

1. The information risk table based on CIA [1: Confidentiality, Integrity and Availability.] criteria.
2. The operational risk table based on ROLFP [2: Reputation, Operational, Legal, Financial and Personal] (see Operational Risks)

Depending selection, the display risk table may change:

Selection	Information Risks	Operational Risks
Root of analysis	All risks of analysis	All risks of analysis
Primary Asset	Risks associated to his supporting assets	Risks associated to himself
Supporting Asset	Risks associated to himself	No risks

4.3.1. Risks table



Home > My Analysis

Risk analysis

Expand all / Wrap all

Search an asset...

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

Assets library

Search an asset...

Department
Department as an entity that regroup persons

Confidentiality: Inherited **Integrity:** Inherited **Availability:** Inherited

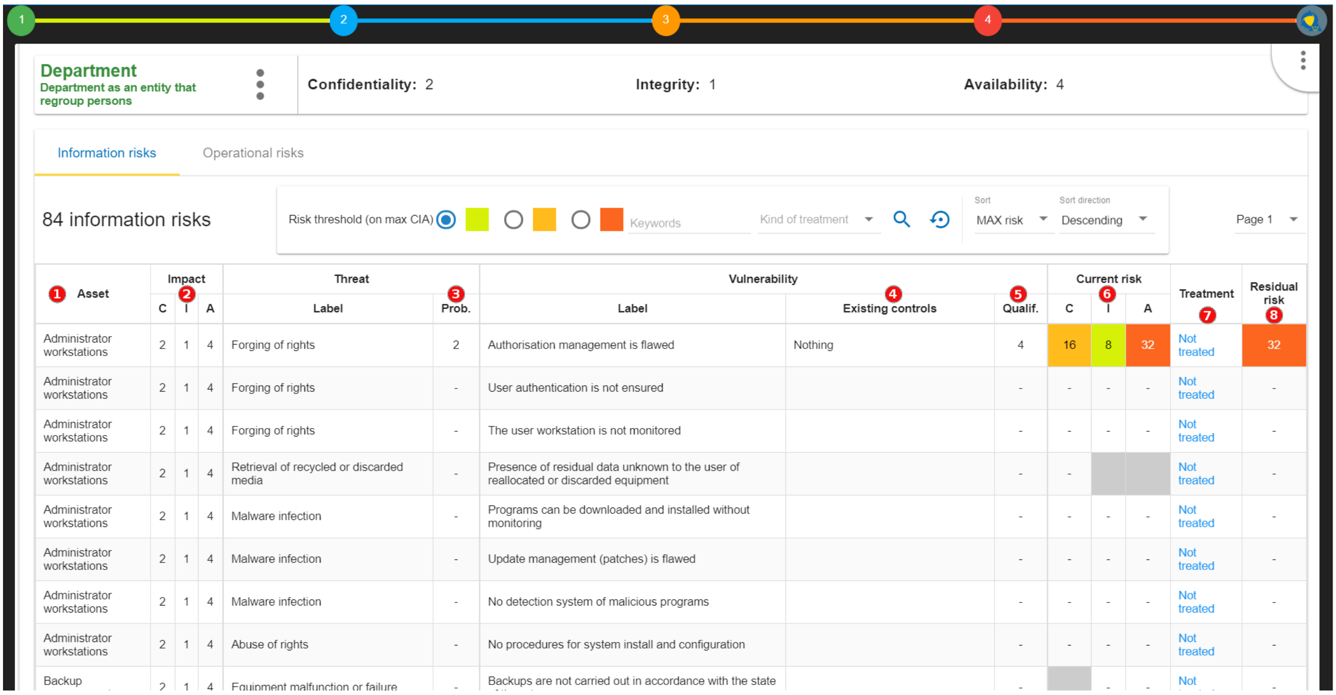
Information risks | Operational risks

84 information risks

Risk threshold (on max CIA) ● 🟩 ○ 🟧 ○ 🟥 Keywords | Kind of treatment | Sort: MAX risk | Sort direction: Descending | Page 1

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Target risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-			Not treated	-
Administrator workstations	-	-	-	Malware infection	-	Programs can be downloaded and installed without monitoring		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Malware infection	-	Update management (patches) is flawed		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Malware infection	-	No detection system of malicious programs		-	-	-	-	Not treated	-
Administrator workstations	-	-	-	Abuse of rights	-	No procedures for system install and configuration		-	-	-	-	Not treated	-
Backup management	-	-	-	Equipment malfunction or failure	-	Backups are not carried out in accordance with the state of the art		-		-	-	Not treated	-

1. The primary asset Department is selected in the analysis.
2. Display the CIA impacts of the Department.
3. Information Risk tab selected.
4. Department asset consists of supporting assets that provide total infomation risks.
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.



Department
Department as an entity that regroup persons

Confidentiality: 2 **Integrity:** 1 **Availability:** 4

Information risks | Operational risks

84 information risks

Risk threshold (on max CIA) ● 🟩 ○ 🟧 ○ 🟥 Keywords | Kind of treatment | Sort: MAX risk | Sort direction: Descending | Page 1

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	2	1	4	Forging of rights	2	Authorisation management is flawed	Nothing	4	16	8	32	Not treated	32
Administrator workstations	2	1	4	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-			Not treated	-
Administrator workstations	2	1	4	Malware infection	-	Programs can be downloaded and installed without monitoring		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Malware infection	-	Update management (patches) is flawed		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Malware infection	-	No detection system of malicious programs		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Abuse of rights	-	No procedures for system install and configuration		-	-	-	-	Not treated	-
Backup	2	1	4	Equipment malfunction or failure	-	Backups are not carried out in accordance with the state		-		-	-	Not	-

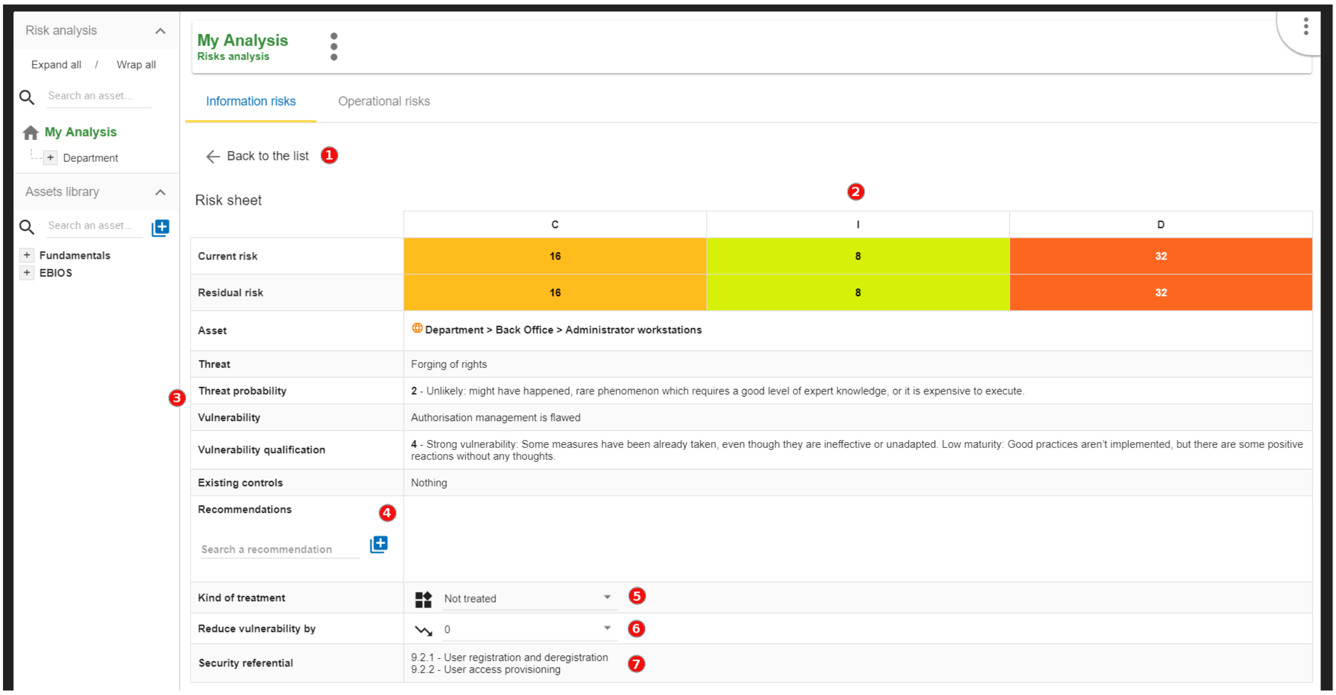
1. Asset: Assets involved in the evaluation.
2. CIA Impact: The CIA criteria that have been assigned to the Department are inherited by default from the supporting assets.

3. Prob: Likelihood of threat (see Scales of threats).
4. Existing controls: Describe, in a factual manner, the security control in place concerning the vulnerability or, more broadly, the risk.
5. Qualif: Evaluation of the control in place in order to determine the level of vulnerability (see Scales of vulnerabilities).
6. Current risk: Risk value calculated according to the risk calculation formula. The colors depend on the risk acceptance grid (see [Risk acceptance thresholds]).
7. Treatment: Indication if the risk is treated, and link to the risk profile (see Risk information sheet).
8. Residual risk: 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 cursor on most fields, a tooltip appears.

4.3.2. Risk information sheet

The risk sheet is displayed when you click on the Not treated link in the information risk table.



Risk sheet

	C	I	D
Current risk	16	8	32
Residual risk	16	8	32
Asset	Department > Back Office > Administrator workstations		
Threat	Forging of rights		
Threat probability	2 - Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.		
Vulnerability	Authorisation management is flawed		
Vulnerability qualification	4 - Strong vulnerability: Some measures have been already taken, even though they are ineffective or unadapted. Low maturity: Good practices aren't implemented, but there are some positive reactions without any thoughts.		
Existing controls	Nothing		
Recommendations Search a recommendation			
Kind of treatment	Not treated		
Reduce vulnerability by	0		
Security referential	9.2.1 - User registration and deregistration 9.2.2 - User access provisioning		

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 recommendations.
5. Selection of kind of treatment:
   a. Reduction / Modification
   b. Denied
   c. Accepted

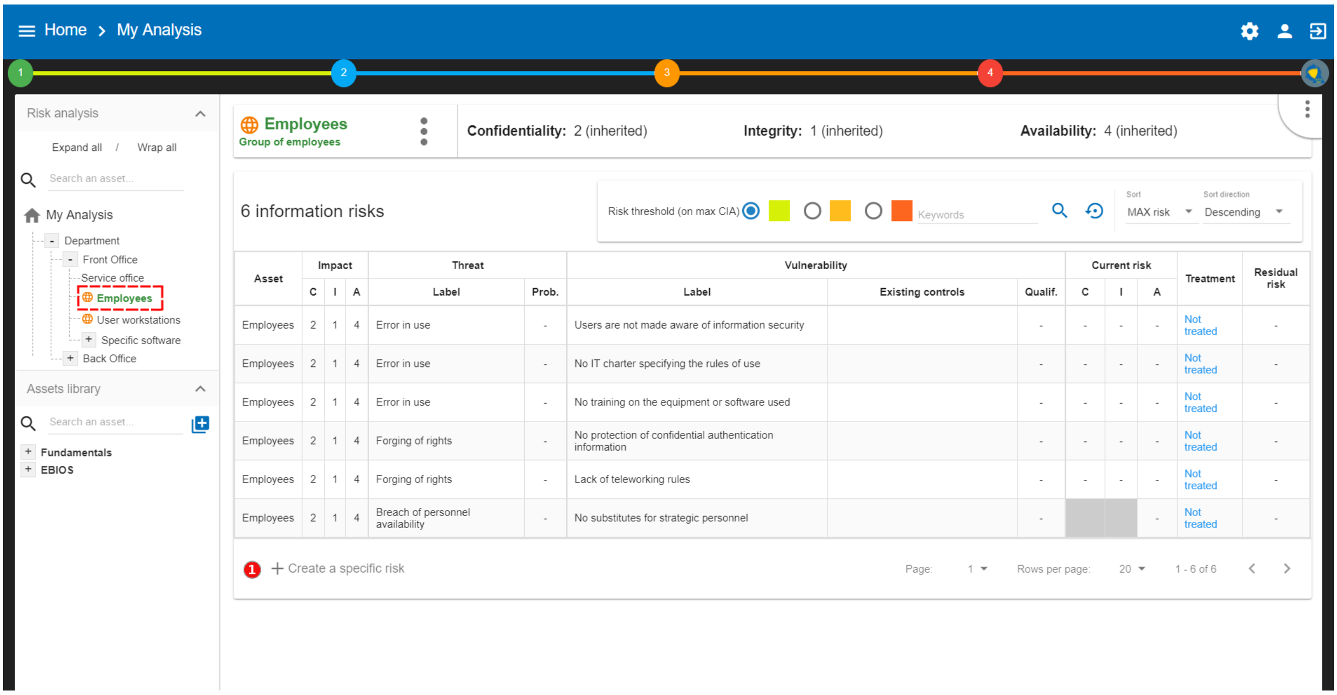
   d. Shared

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.

Don’t forget to save the form in order to calculate the residual risk.

4.3.3. Adding additional risk

When an asset is selected in the analysis:



Employees
Group of employees

Confidentiality: 2 (inherited) **Integrity:** 1 (inherited) **Availability:** 4 (inherited)

6 information risks

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

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		
Employees	2	1	4	Error in use	-	Users are not made aware of information security		-	-	-	-	Not treated	-
Employees	2	1	4	Error in use	-	No IT charter specifying the rules of use		-	-	-	-	Not treated	-
Employees	2	1	4	Error in use	-	No training on the equipment or software used		-	-	-	-	Not treated	-
Employees	2	1	4	Forging of rights	-	No protection of confidential authentication information		-	-	-	-	Not treated	-
Employees	2	1	4	Forging of rights	-	Lack of teleworking rules		-	-	-	-	Not treated	-
Employees	2	1	4	Breach of personnel availability	-	No substitutes for strategic personnel		-			-	Not treated	-

1 + Create a specific risk

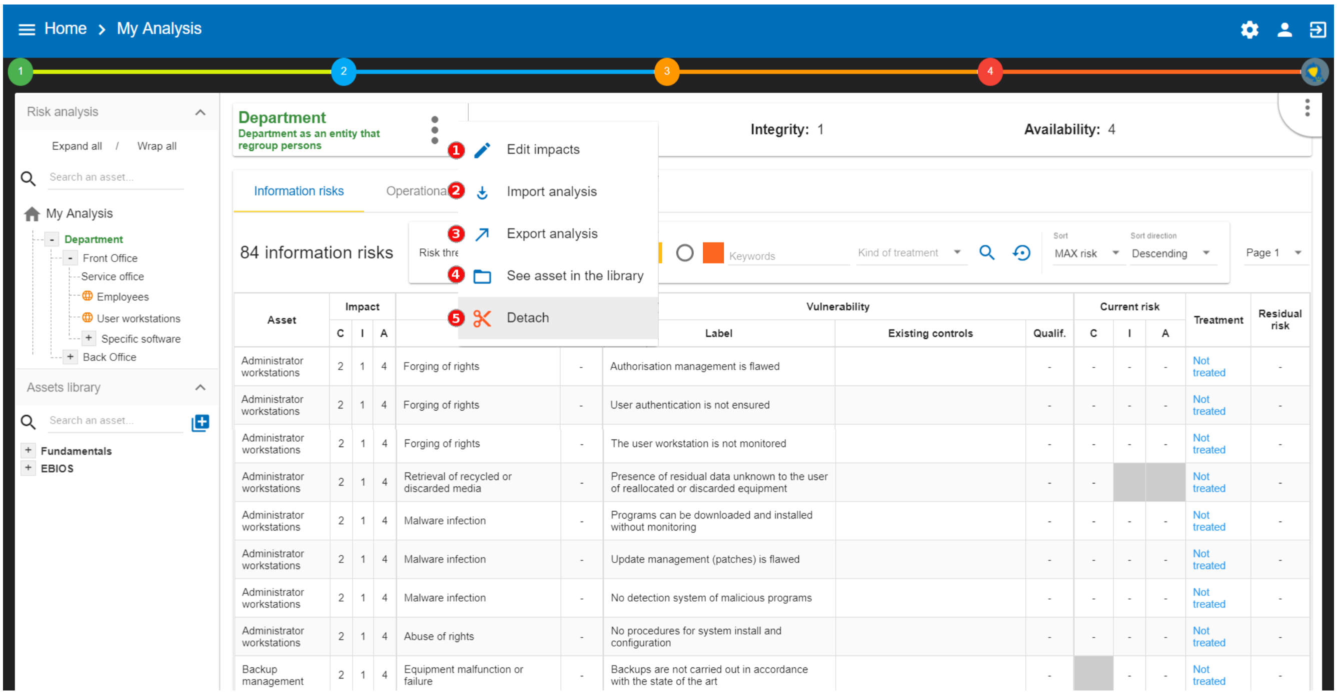
Page: 1 Rows per page: 20 1 - 6 of 6

1. Click to `create a specific risk`: A pop-up appears and allows to associate a threat and vulnerability pair with the current asset.

Threat and vulnerability must exist beforehand.

4.3.4. Contextual menu of asset

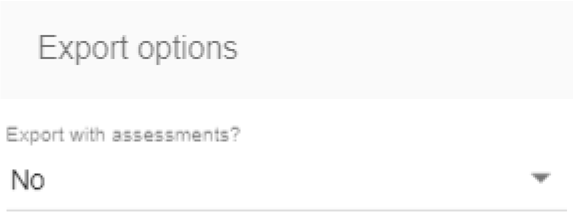
By clicking on ⋮, the context menu of asset appears:



Asset	Impact					Vulnerability			Current risk			Treatment	Residual risk
	C	I	A			Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	2	1	4	Forging of rights	-	Authorisation management is flawed		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Forging of rights	-	User authentication is not ensured		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Forging of rights	-	The user workstation is not monitored		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment		-	-			Not treated	-
Administrator workstations	2	1	4	Malware infection	-	Programs can be downloaded and installed without monitoring		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Malware infection	-	Update management (patches) is flawed		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Malware infection	-	No detection system of malicious programs		-	-	-	-	Not treated	-
Administrator workstations	2	1	4	Abuse of rights	-	No procedures for system install and configuration		-	-	-	-	Not treated	-
Backup management	2	1	4	Equipment malfunction or failure	-	Backups are not carried out in accordance with the state of the art		-		-	-	Not treated	-

1. `Edit impacts`: Displays the impact and consequence modification view (see Impacts and consequences).
2. `Import analysis`: 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 Importing an asset).
3. `Export analysis`: Allows you to export an analysis, from the place pointed by the selected asset of the analysis. The export works exactly like exporting an asset, see Exporting an asset).

> The additional option, `export with assessment`. It means, export gets the evaluation and treatment of risks. By default is disable.


Export options

Export with assessments?
No

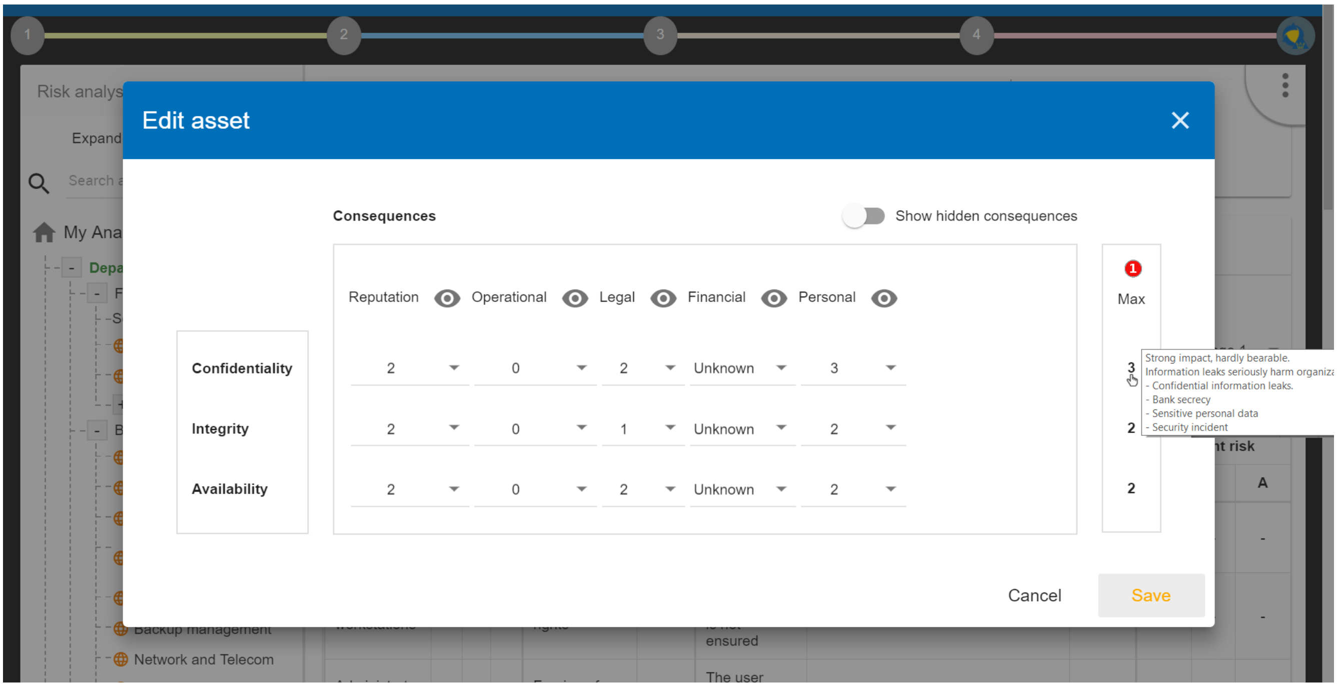
4. `See asset in the library`: Displays the asset from the library, allowing you to have another context menu that allows changes to the asset. (see Context menu of library)
5. `Detach` : This removes an asset from the risk analysis.

> This action may lead to the loss of risk assessments for this asset and its children.

4.3.5. 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.



Consequences ○ Show hidden consequences

	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

Strong impact, hardly bearable.
Information leaks seriously harm organiza
- Confidential information leaks.
- Bank secrecy
- Sensitive personal data
- Security incident

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.

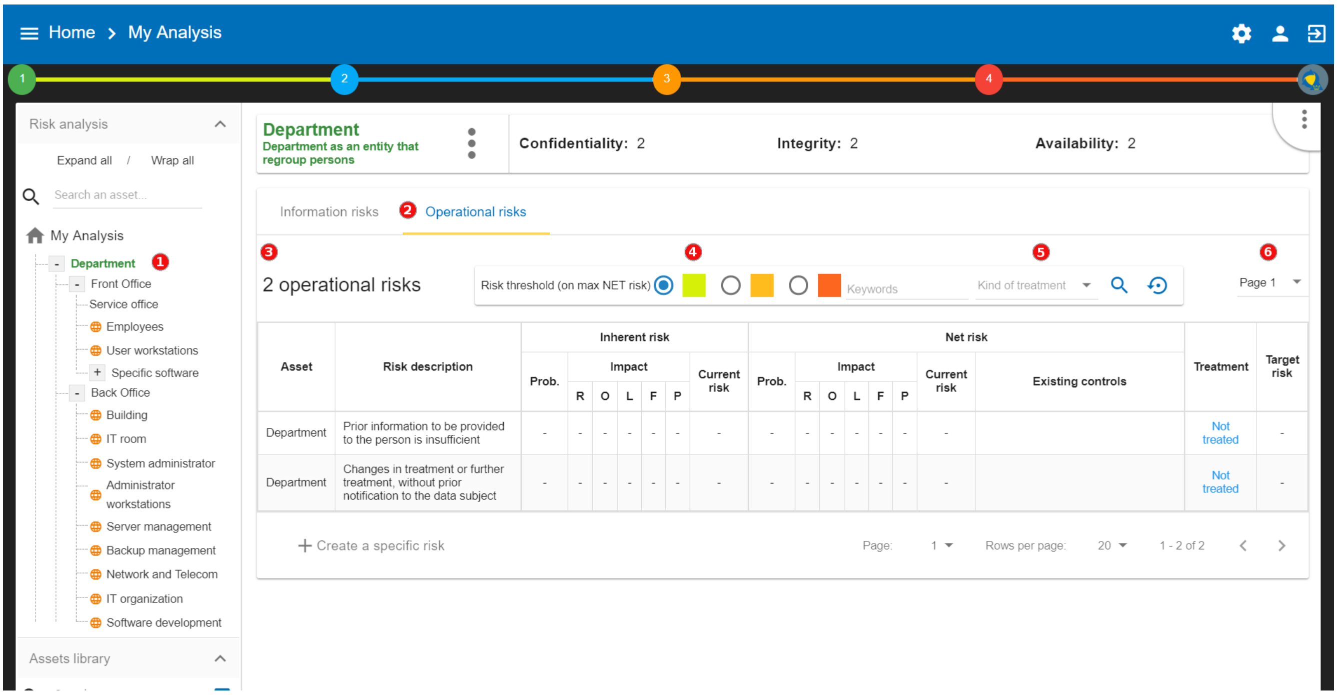
When one of the criteria **C** (confidentiality), **I** (integrity) or **A** (availability) is allocated, there is a need to ask : what are the consequences on the company, and more particularly on its ROLFP, i.e. its **R**eputation, its **O**peration, its **L**egal, its **F**inances or the impact on 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.

To hide the consequences that won't consider. Click on icon 👁. To show it again. Click on `Show hidden consequences`

4.4. Operational Risks

4.4.1. Risks table



Department
Department as an entity that regroup persons

Confidentiality: 2 Integrity: 2 Availability: 2

2 operational risks

Risk threshold (on max NET risk) ● 🟩 ○ 🟨 ○ 🟥

		Inherent risk							Net risk									
Asset	Risk description	Prob.	Impact					Current risk	Prob.	Impact					Current risk	Existing controls	Treatment	Target risk
			R	O	L	F	P			R	O	L	F	P				
Department	Prior information to be provided to the person is insufficient	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not treated	-
Department	Changes in treatment or further treatment, without prior notification to the data subject	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not treated	-

Page: 1 Rows per page: 20 1 - 2 of 2

1. Select the primary asset. In this case, `Department`.
2. Click on tab `Operational risks`.
3. Total of operational risks associated to primary asset.
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.

The operational risk table may or may not display the inherent risks. They are the operational risks that would impact the organization without any controls in place. To show this option see Creating a Risk Analysis.

[Fields Operational Risk Table]

1. `Asset`: Assets involved in the evaluation
2. `Risk description`: Description of risk
3. `Inherent risk`: Operational risk is calculated from the two factors, the probability (`Prob.`) of the risk scenario and the `Impact` based on the ROLFP [2: Reputation, Operational, Legal, Financial and Personal] without controls in place. The current risk represents the maximum value of the probability on the ROLFP impact values.
4. `Net risk`: Net risk represents the risk with the measures currently in place. The calculation is the same as for the inherent risks.
5. `Existing controls`: Describe here, in a factual manner, the control in place.
6. `Treatment`: Indication if the risk is treated and risk profile (see Operational risk sheet).
7. `Residual risk` : 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.

4.4.2. 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 :
   a. Modification / Reduce
   b. Refused
   c. Accepted
   d. Shared
7. Saving the form in order to calculate the residual risk

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

4.4.3. 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.

5. 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

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

5.1. 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).

5.2. 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).

5.3. 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).

5.4. 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.

6. 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.

6.1. 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.

6.2. 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.

6.3. 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.

6.4. ISO 27002 controls

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

6.5. 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.

6.6. 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.

6.7. 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.

7. 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
3. Click to encode a new interview
4. Information to be entered: date, names of persons and possibly subjects covered.

8. 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:
    a. View a Snapshot
    b. Restore Snapshot. Caution this option will overwrite the current analysis.
    c. 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.

9. 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