



OPTIMISED RISK ANALYSIS

[www.monarc.lu](http://www.monarc.lu)

# User Guide

CASES Luxembourg

Version 2018-05-09

# Table of Contents

1. Introduction .....	1
1.1. Purpose .....	1
1.2. Other documents .....	1
1.3. Syntax used in the document .....	1
1.4. Syntax used in MONARC .....	1
2. Home Page .....	2
2.1. Dashboard .....	2
2.2. Creating a Risk Analysis .....	2
2.3. Main risk analysis view .....	3
3. Client Environment Administration .....	5
3.1. Administration .....	5
4. Analysis Management .....	13
4.1. Method steps call .....	13
4.2. Library .....	14
4.3. Information Risks .....	22
4.4. Operational Risks .....	28
5. Evaluation Scales .....	32
5.1. Impact scale .....	33
5.2. Likelihood scale .....	33
5.3. Vulnerability scale .....	34
5.4. Acceptance thresholds .....	34
6. Management of Knowledge Base .....	36
6.1. Type of assets .....	37
6.2. Threats .....	37
6.3. Vulnerabilities .....	38
6.4. ISO 27002 controls .....	38
6.5. Risks .....	38
6.6. Tags (Operational Risks) .....	38
6.7. Operational Risks .....	38
7. Interviews .....	39
8. Snapshots .....	41
9. Managing the Implementation Treatment Plan .....	43

# 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



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. e.g. 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.



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

## 2. Home Page

### 2.1. Dashboard

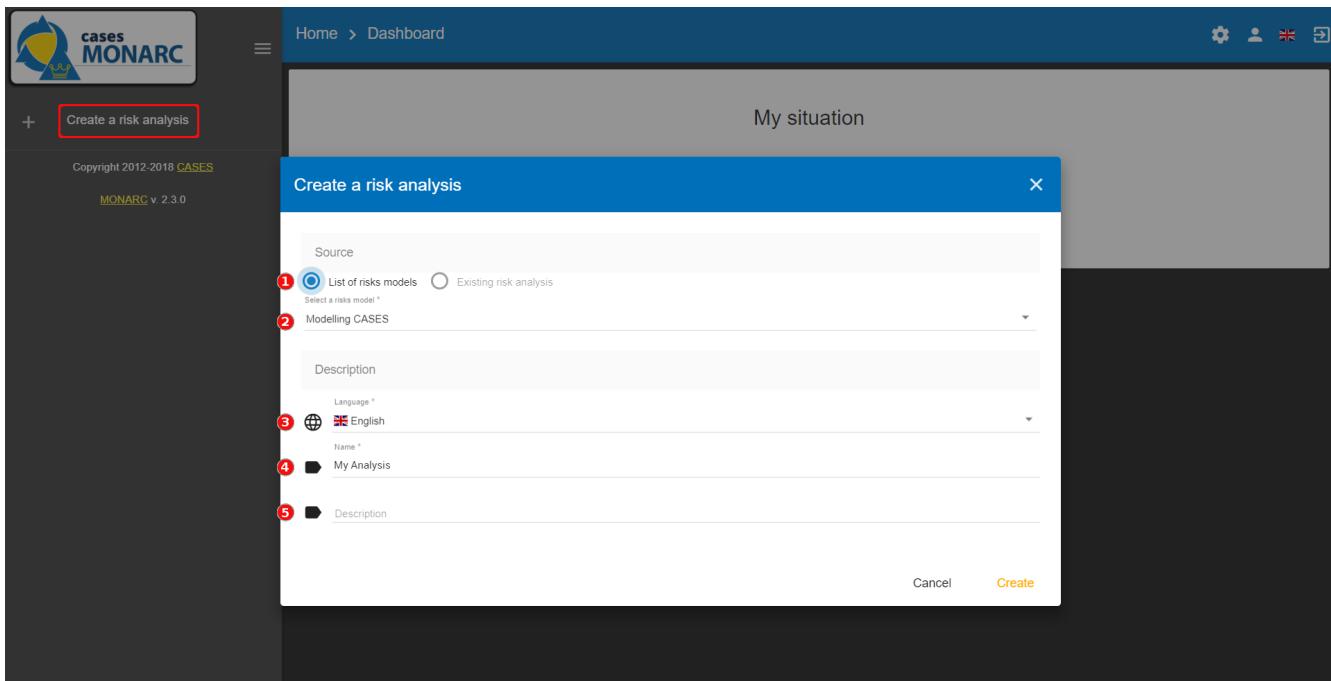
Immediately after user authentication, the following screen appears. It may, however, be slightly different, if there is not yet an analysis created or if there are already several and according to the state of progress of the analysis.

The screenshot shows the MONARC Home Page Dashboard. On the left, there is a sidebar with the MONARC logo, navigation links for 'My Analysis' (with a red notification dot) and 'Create a risk analysis' (with a red notification dot), and copyright information. The main content area is titled 'My situation' and contains two sections: 'Current risks map' and 'Target risks map'. The 'Current risks map' is a 5x5 grid where each cell represents a risk level from 0 to 4. A red dot labeled '1' is positioned over the cell at row 4, column 15. Below the grid, three horizontal bars indicate the count of risks: '0 low risks' (green bar), '0 medium risks' (orange bar), and '1 high risks' (red bar). The 'Target risks map' section displays a message: 'No target risks specified in your risk analysis yet.' At the top right of the dashboard, there are icons for administration, account, interface language, and logout.

1. Graph showing the statistics of the last modified risk analysis.
2. List of existing analyses. 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 [Administration](#), [Account](#), [Interface language](#) or [Logout](#) (see [Client Environment Administration](#)).

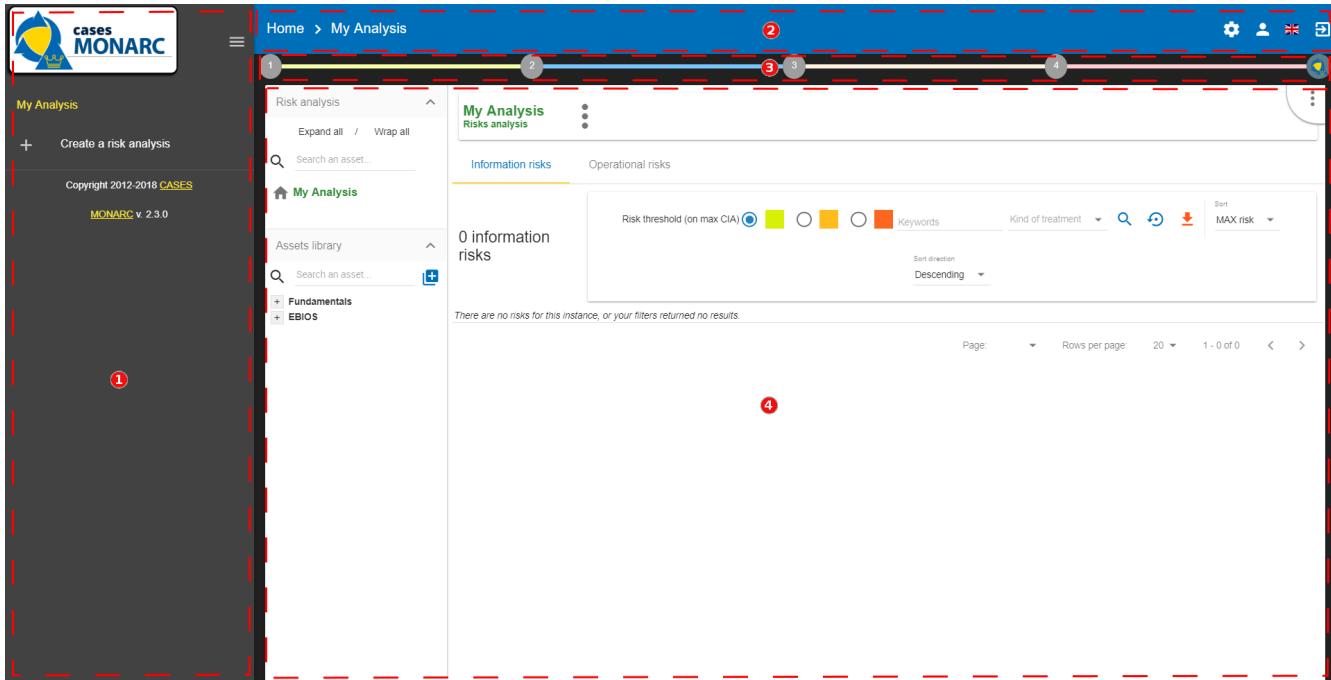
### 2.2. Creating a Risk Analysis

After clicking on [Create a risk analysis](#), the following pop-up appears



1. The creation of a risk analysis is always based on an existing model. There are two choices for this:
  - a. **List of risks models:** 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 risk analysis of your choice present in your environment.
2. Options **a** or **b** before being selected. It gets the source.
3. Select the preferred language for this new risk analysis. MONARC only present the languages actually available in the selected source.
4. Give a name to risk analysis.
5. Optional field, which allows you to describe your analysis in more detail.

## 2.3. Main risk analysis view



## 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 .

2. Navigation panel: User administration and account management.
3. Access to the steps of the method by clicking on numbers 1 to 4.
4. 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.



## 1. Administration (Enable only for administrator users)

- Manage users (see [Manage users](#))
- Organization (see [Organization](#))
- Deliverable templates (see [Deliverable templates](#))

## 2. User account (see [User account](#))

## 3. Interface language (see [Interface language](#))

## 4. Logout

## 3.1. Administration

### 3.1.1. Manage users

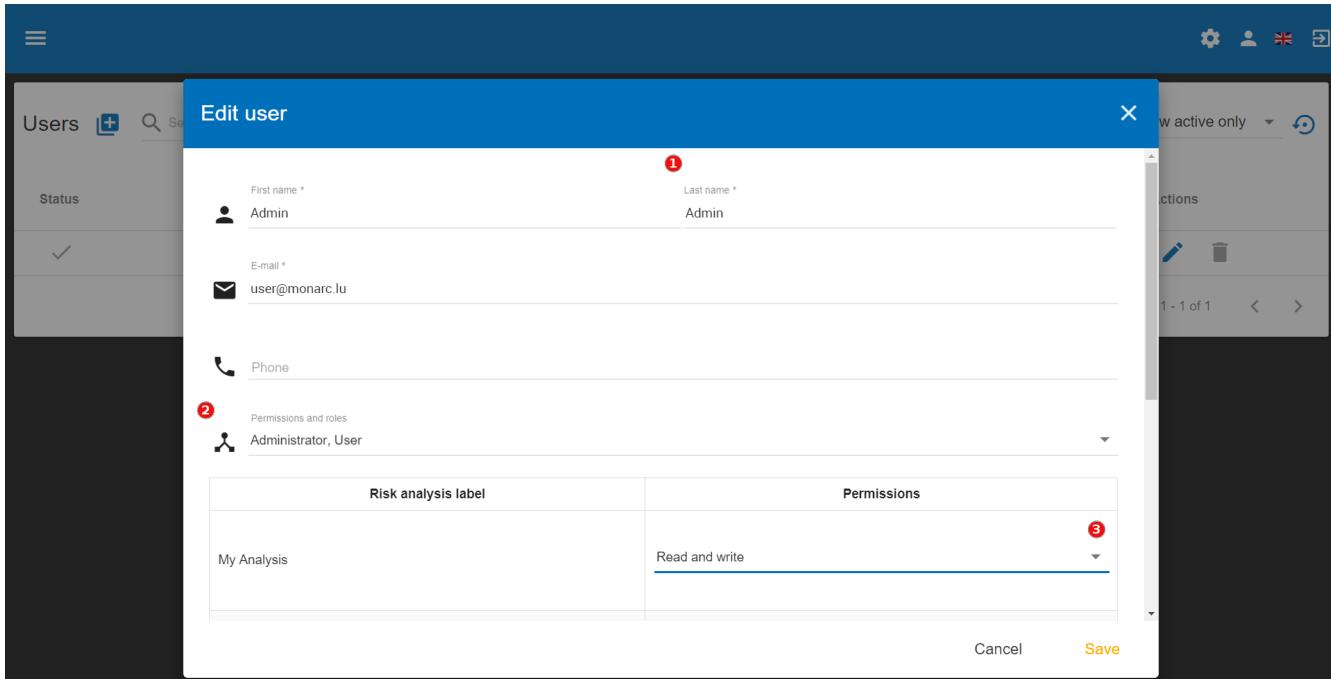
#### List of users

Status	First name	Last name	E-mail	Phone	Actions
<input checked="" type="checkbox"/> ②	Admin	Admin	user@monarc.lu		④  ⑤

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 on the icon  , the following screen appears:



The screenshot shows the 'Edit user' dialog box over a 'Users' list. The dialog contains the following fields:

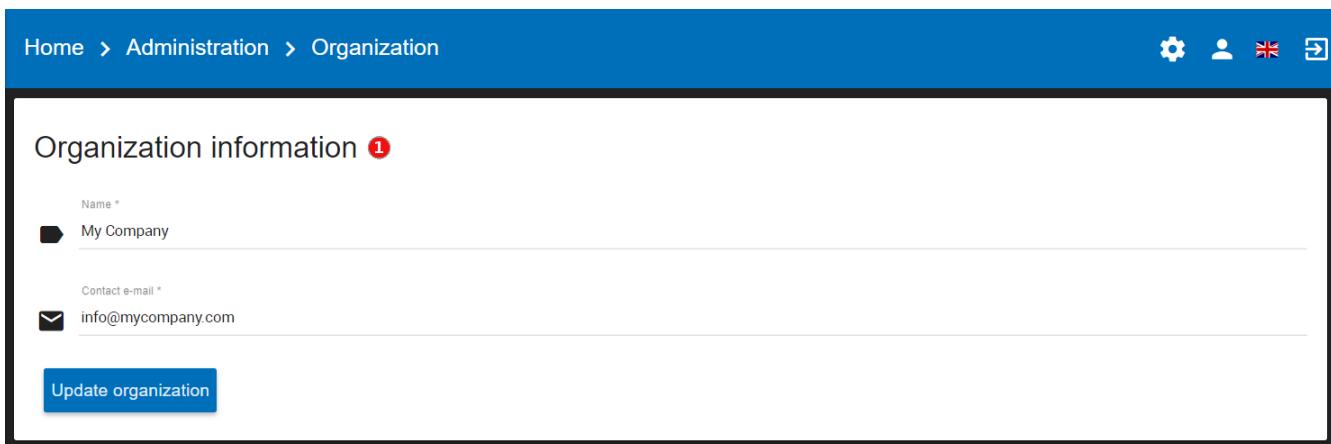
- General Information:**
  - First name \*: Admin (with a red circled '1' icon)
  - Last name \*: Admin
  - E-mail \*: user@monarc.lu
  - Phone: (empty)
- Permissions and roles:**
  - Administrator, User (with a red circled '2' icon)
- Risk analysis label:**

Risk analysis label	Permissions
My Analysis	Read and write (with a red circled '3' icon)

At the bottom right are 'Cancel' and 'Save' buttons.

1. General information.
2. Selection of profiles **Administrator** or/and **User**.
3. Management of user rights by analysis. By risk analysis, there are 3 types of rights:
  - No access.
  - Read only.
  - Read and write.

### 3.1.2. Organization



The screenshot shows the 'Organization information' dialog box. It contains the following fields:

- Name \*: My Company (with a red circled '1' icon)
- Contact e-mail \*: info@mycompany.com

At the bottom is a blue 'Update organization' button.

1. Manage general information about the entity (MONARC account).

### 3.1.3. Deliverable templates

It's possible with MONARC to custom by organization the different deliveries which are generated.

This view summarizes all the available templates. There are some actions available on template :

1. **Download** a template.
2. **Edit** a template. The view for editing a template is the same as one for adding one. This view is explained below.
3. **Delete** a template. This action permanently delete the template for all the users of the company.



The default template are only downloadable, they can't be modified or deleted.

4. **Add a new template :**

This view summarizes all the available templates. There are some actions available on template :

1. Select the **Category** of the template. The category is linked to the different step of the method.
2. Select the **Language** associated to the template and the next description to fill.

3. Fill the **Description** of the new template.
4. Click on the grey area or drag and drop a document on the grey area to **Upload** the template.



You don't have to fill all the languages, one language is sufficient.

## List of tags

MONARC allows you to add your deliveries template. The template is a document which use different tags.



All the deliveries in MONARC have to be set in Word Format (.docx)

### List of tags for the layout of the document:

All these tags are mainly set in the form depending of the delivery.

Current risk			Treatment	Residual risk
C	I	A		
30	30	45	Not treated	45
		20	Reduction	6
20		30	Reduction	6
18	18	24	Reduction	0
18		24	Reduction	0
16	16	24	Reduction	18
		24	Not treated	24

1.  **\${STATE}** : State of the document with prefilled value (draft or final).
2.  **\${VERSION}** : Version of the document.
3.  **\${CLASSIFICATION}** : Classification of the document.
4.  **\${DOCUMENT}** : Name of the document.
5.  **\${CLIENT}** : Name of the customer.
6.  **\${SMILE}** : Name of the security consultant who do the analysis.

There are also two others tags which are generated by the application :

- **\${COMPANY}** : Name of the company which come from MONARC, it's stored in the database and editable in the application.
- **\${DATE}** : Date of the generation of the document. Field auto-generated by MONARC.

## List of the tags from the context establishment:

The screenshot shows the MONARC software interface. At the top, there's a navigation bar with 'Home' and 'My Print'. Below it is a search bar with 'Risks analysis context' (1) checked. The main area is titled 'Context Establishment' and contains several checkboxes: 'Evaluation of Trends and Threat, and synthesis' (2), 'Risks management organisation' (3), and 'Definition of the risk evaluation criteria' (4). To the right, there's a table titled 'Operational risks' with 138 information risks listed. The table has columns for Asset, Threat, Vulnerability, Existing controls, Current risk, Treatment, and Residual risk. Various filters like 'Risk threshold (on max CIA)' and 'Sort direction' are also present.

1. \${CONTEXT\_ANA\_RISK}: Free text which comes from the step: "Risk analysis context".
2. List of the tags from "Evaluation of Trends and Threat, and synthesis":
  - \${SYNTH\_EVAL\_THREAT}: The summary of the step: "Evaluation of Trends and Threat, and synthesis".
  - \${TABLE\_THREATS}: A summary of the threat assessment.
  - \${TABLE\_EVAL\_TEND}: The trend assessment with the questions which are answered.
  - \${TABLE\_THREATS\_FULL}: The full threat assessment.
3. \${CONTEXT\_GEST\_RISK}: Free text which comes from the step: "Risk management organization".
4. List of the tags from "Definition of the risk evaluation criteria":
  - \${SCALE\_IMPACT}: The table of the impact scale.
  - \${SCALE\_THREAT}: The table of the threats scale.
  - \${SCALE\_VULN}: The table of the vulnerabilities scale.
  - \${TABLE\_RISKS}: The table of the information risk acceptance threshold.

## List of tags for the context modelling:

1. \${SYNTH\_ACTIF}: Free text which comes from the step: “synthesis of assets/impacts”.
- \${IMPACTS\_APPRECIATION}: A table which is generated by MONARC. It represents the impacts/consequences of the top level assets.

#### List of the tags for the Evaluation and treatment of risks:

1. \${SUMMARY\_EVAL\_RISK}: Free text which comes from the form.

#### List of the tags generated by MONARC :

- \${CURRENT\_RISK\_MAP}: Table which represents the distribution of the current risks.
- \${TARGET\_RISK\_MAP}: Table which represents the distribution of the targeted risks.
- \${DISTRIB\_EVAL\_RISK}: A text which represents the distribution of the risks by levels.

- \${GRAPH\_EVAL\_RISK}: A graph which represents the \${DISTRIB\_EVAL\_RISK}
- \${RISKS\_RECO\_FULL}: A table which represents the recommendation for the information risks
- \${OPRISKS\_RECO\_FULL}: A table which represents the recommendation for the operational risks
- \${TABLE\_AUDIT\_INSTANCES}: A table with all the informational risks.
- \${TABLE\_AUDIT\_RISKS\_OP}: A table with all the operational risks.

#### List of the tags for Implementation and monitoring:

List of tags generated by MONARC :

- \${TABLE\_IMPLEMENTATION\_PLAN}: Table which shows all the recommendations to implement.
- \${TABLE\_IMPLEMENTATION\_HISTORY}: Table which shows all the implemented recommendations.

#### List of the tags for the annexes:

Some tags are linked to other functionality of MONARC like:

- \${TABLE\_INTERVIEW}: The list of all the interviews.

### 3.1.4. User account

This view allows you to:

My account

1 Personal information

First name: Admin

Last name: Admin

E-mail: user@monarc.lu

2 Change password

Current password

New password

Confirm new password

Update password

1. Manage general user information.
2. Change the password. Password complexity is required.

### 3.1.5. Interface language

There are 4 interface language:

- French
- English
- German
- Dutch



This action only changes the interfaces language (The risk analysis language is not modified).

# 4. Analysis Management

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

The screenshot shows the MONARC Risk Analysis interface. A red dashed box highlights the main work area. Four numbers (1, 2, 3, 4) are placed around the interface to indicate different sections:

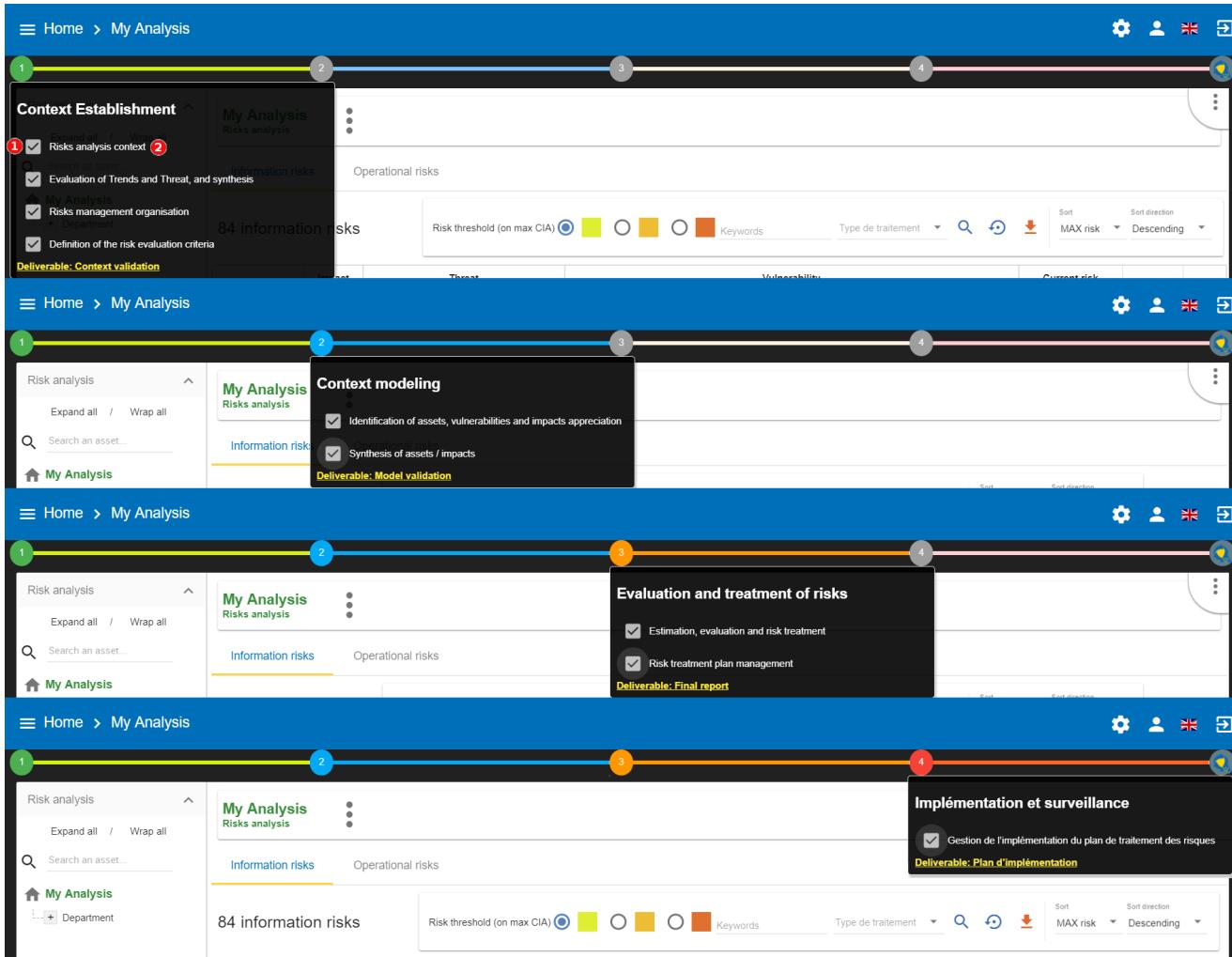
- 1**: Located at the top center, above the main menu bar.
- 2**: Located on the left side, next to the 'Assets library' section.
- 3**: Located on the left side, next to the 'My Analysis' section.
- 4**: Located at the bottom right of the main work area.

The main work area displays a table of 'Information risks' (84 rows). The columns include Asset, Impact (C, I, A), Threat, Label, Prob., Vulnerability, Existing controls, Qualif., Current risk (C, I, A), Treatment, and Target risk. The 'Treatment' column contains several cells with a gray background and white text, indicating '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 call](#)).
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 call

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



1. Ticking 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.

The screenshot shows the MONARC software interface. On the left, there's a sidebar with a search bar, a 'My Analysis' button, and a 'Assets library' section containing a search bar and a 'Fundamentals' category. The 'Fundamentals' category is expanded, showing 'Primary Assets' (with 4 items), 'Model Structure', 'Backup', and 'Buildings & Premises'. Under 'Buildings & Premises', there are icons for 'Company premises', 'Archive room' (marked with a red circle and number 5), 'IT room', 'Building', and 'Service office'. Below these are sections for 'Physical Goods', 'Software', 'Equipment', 'Staff', 'Organization', 'Servers', 'Network', and 'GDPR'. The 'EBIOS' section is collapsed. On the right, the main area is titled 'My Analysis Risks analysis' and shows 'Information risks' and 'Operational risks' tabs. The 'Information risks' tab is selected, displaying '84 information risks'. Below this is a table with columns for Asset, Impact (C, I, A), Threat (Label, Prob.), Vulnerability (Label, Existing controls, Qualif.), Current risk (C, I, A), Treatment, and Target risk. Several rows of data are listed, such as 'Administrator workstations' with 'Forging of rights' and 'Malware infection' threats.

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 to 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**.

1. Asset management context menu (details in [Context menu of library](#)).
2. Add an existing asset in the structure, creating a composed asset. There is no limit to 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**.

The screenshot shows the MONARC user interface with the following details:

- Top Navigation:** Home > My Analysis > Library.
- Progress Bar:** A horizontal bar at the top with four segments: green (1), blue (2), orange (3), and red (4).
- Left Sidebar:** Contains search bars for 'Search an asset...', 'My Analysis', and 'Assets library'. Below these are tree-based navigation sections for 'Fundamentals' (Primary Assets, Model Structure, Backup, Buildings & Premises, Company premises, Archive room, IT room, Building, Service office), 'Physical Goods' (Software, Equipment, Staff, Organization, Servers), and 'Organizations' (Organizations).
- Asset Card:** The central card is for a 'Building' asset. It includes:
  - Composition:** Shows it is part of the 'Back Office' (3).
  - Asset used in the risks analysis:** Shows it is an 'Active parent' of 'My Analysis > Building > Back Office > Department' (4).
  - 5 information risks:** A table with two rows:
 

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
- Actions:** Includes a delete icon with a count of 5 (5).

1. Asset management context menu (details in [Context menu of library](#)).
2. Add an existing asset in the structure, creating a compound asset. There is no limit to 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.

The screenshot shows the MONARC user interface. At the top, there's a navigation bar with 'Home > My Analysis > Library'. Below the navigation is a toolbar with four colored circles (green, blue, orange, red) and some icons. On the left, there's a sidebar with sections for 'Risk analysis' (with 'Expand all / Wrap all' buttons), 'My Analysis' (with 'Department' button), 'Assets library' (with 'Search an asset...' input), and a tree view for 'Fundamentals' (including 'Primary Assets', 'Model Structure', 'Backup', 'Buildings & Premises' which is expanded to show 'Company premises', 'Archive room', 'IT room', and 'Building' which is selected and shown as 'Service office'). The main content area shows 'Asset used in the risks analysis' with a table and an 'Actions' column containing a delete icon. Below that is a section for '5 information risks' with a table.

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 #)**, 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 icon , the following pop-up appears:

The screenshot shows the 'Add an asset' dialog box. It has tabs for 'Labels and descriptions' (with 'Name \*' and 'Label \*' fields, both marked with red numbers 2 and 3), 'General information' (with 'Scope' dropdown set to 'Local' marked with red number 4), and 'Operational risk Tag' (with 'Category \*' dropdown set to 'INFO - Information' marked with red number 5). There are also 'Location' and 'Abuse of rights' sections. At the bottom, there are 'Cancel', 'Create', and 'Create and continue' buttons. In the background, the library list shows various assets like 'Administrator workstations', 'Backup management', and 'Building'.

1. To create an asset, it is also possible to import it (see [Importing an asset](#)).
2. **Name**: This name must be unique for the analysis.
3. **Label**: This is an additional description, it is displayed in the tooltip when the mouse is positioned without moving on the asset.
4. **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 of the primary asset can change the level of risk.

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



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

8. **Location**: Allows you to order assets in the selected category.

#### 4.2.4. Edit an asset

The call is made from the [Context menu of library](#) 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:

- **Scope**
- **Asset type**

#### 4.2.5. Importing an asset

This pop-up is accessible from the pop-up [Add a new asset](#) 

The screenshot shows the MONARC application interface. At the top, there's a navigation bar with 'Home > My Analysis'. Below it is a toolbar with four colored circles (green, blue, orange, red) and some icons. On the left, there's a sidebar with sections like 'Risk analysis', 'Department' (selected), 'Assets library', and 'Fundamentals/EBIOS'. The main area shows a table of risks with columns for 'Information risks' and 'Operational risks'. A modal window titled 'Asset import center' is open in the foreground. It contains an 'Import method:' section with two options: 'By duplicating' (radio button) and 'By merging' (radio button, highlighted with a red circle). A note below says 'Only global assets can be imported by merge.' There are two buttons at the bottom of the modal: 'Import from file' (highlighted with a red circle) and 'Import from MONARC library' (also with a red circle). A 'Cancel' button is in the bottom right corner of the modal.

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 merging.

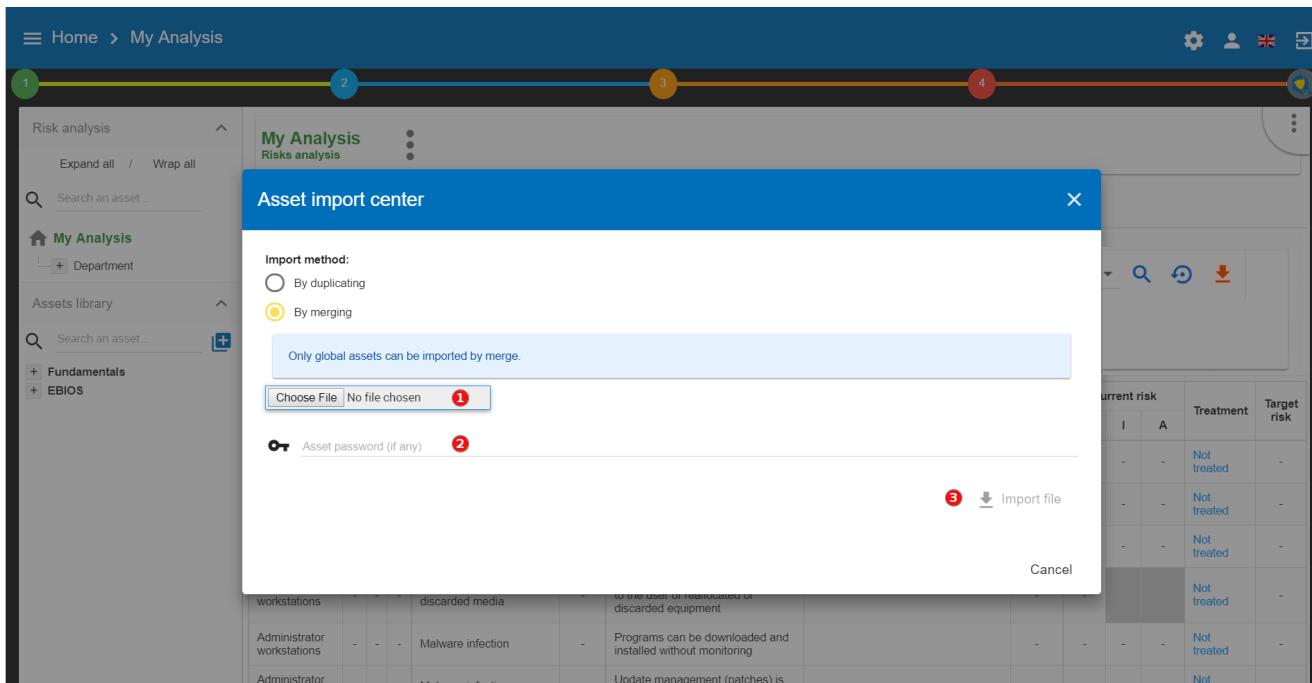
2. **Import from file:** allows to exchange assets from one environment to another (see [Importing an asset from a file](#)).
3. **Import from MONARC library:** This option is not available in the case of a *Stand alone* version of MONARC (see [Import from the MONARC library](#)).



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

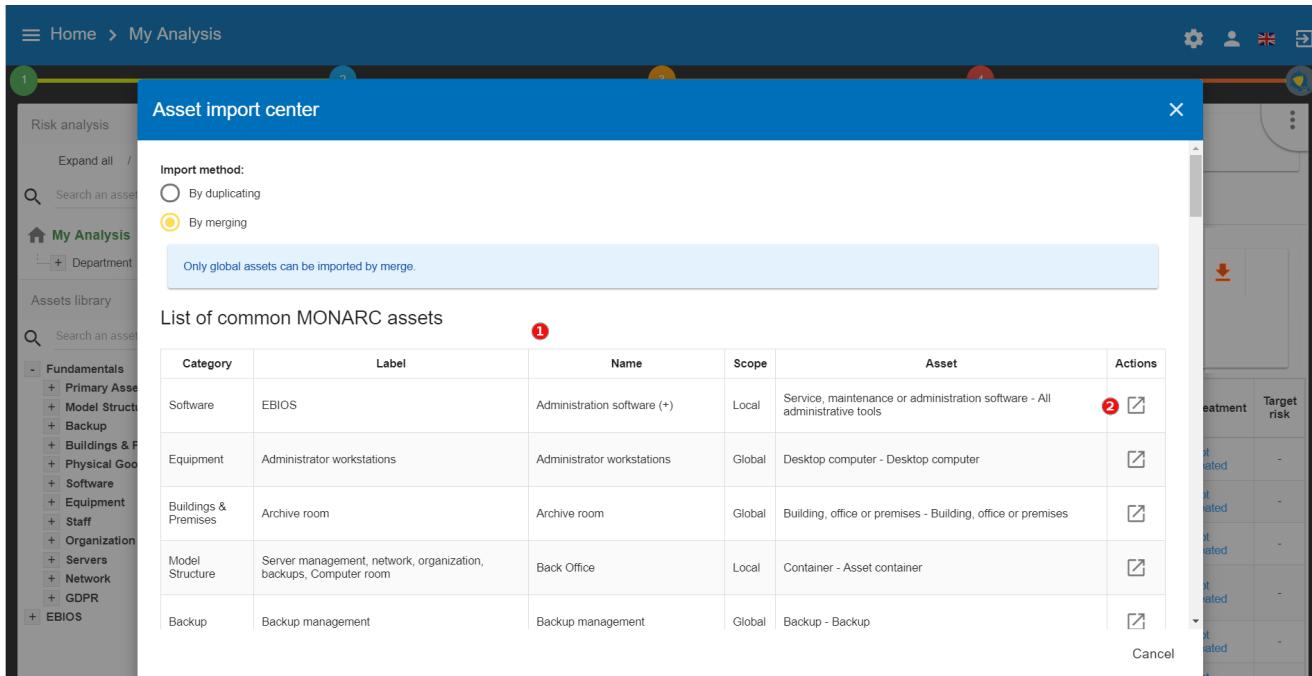
The pop-up appears after clicking on the **Import from file** option in the **Asset Import center**.



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**.



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

The screenshot shows the MONARC interface with a navigation bar at the top. The main area displays a tree view of assets under 'My Analysis' and a table of '5 information risks'. A modal dialog box is open in the center, titled 'Export asset'. It contains a section for 'Encryption' with two radio button options: 'Custom password' (selected) and 'Without password'. Each option has a red circle with a number: '1' for 'Custom password' and '2' for 'Without password'. At the bottom of the dialog are 'Cancel' and 'Export' buttons.

1. **Custom password:** Possibility to encrypt the generated JSON file with a symmetric password that will be necessary during the import.
2. **Without password:** JSON file decoded.

## 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:

The screenshot shows the MONARC interface with a navigation bar at the top. The main area displays a tree view of assets under 'My Analysis' and two risk tables: 'Information risks' and 'Operational risks'. The 'Information risks' table is selected and displayed prominently, showing 84 risks. The table has columns for Asset, Impact (C, I, A), Threat, Vulnerability (Label, Existing controls, Qualif.), Current risk (C, I, A), Treatment, and Target risk. The 'Operational risks' table is also visible below the 'Information risks' table.

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 with his supporting assets	Risks associated with himself
Supporting Asset	Risks associated with himself	No risks

#### 4.3.1. Risks table

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 information risks.
5. Possibility to select only certain risks according to the risk acceptance threshold.
6. Ability to sort of most columns of the table.

① Asset	Impact			③ Prob. Label	Vulnerability			⑤ Qualif.	Current risk			Treatment	⑧ Residual risk
	C	I	A		Label	④ Existing controls	⑥ 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 [Likelihood scale](#)).
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 control in place in order to determine the level of vulnerability (see [Vulnerability scale](#)).
6. **Current risk:** Risk value calculated according to the risk calculation formula. The colours depend on the risk acceptance grid (see [Acceptance thresholds](#)).
7. **Treatment:** Indication if the risk is treated, and links 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 the cursor in 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. Reminders of the parameters of the risk table.
4. Creation / Assignment button for one or more recommendations.
5. Selection of the 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. Proposals of controls, which come from various repositories.



Do not 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:

The screenshot shows the MONARC application interface. At the top, there's a navigation bar with 'Home > My Analysis'. Below it is a horizontal progress bar with four colored segments: green (1), blue (2), orange (3), and red (4). The main content area is titled 'Employees Group of employees'. It shows 'Confidentiality: 2 (inherited)', 'Integrity: 1 (inherited)', and 'Availability: 4 (inherited)'. On the left, there's a sidebar with 'My Analysis' and 'Assets library' sections. The 'My Analysis' section has a tree view where 'Employees' is selected and highlighted with a red box. The 'Assets library' section lists 'Fundamentals' and 'EBIOS'. The central part of the screen shows a table titled '6 information risks' with columns for Asset, Impact, Threat, Vulnerability, Current risk, Treatment, and Residual risk. Each row corresponds to a specific risk for the 'Employees' asset.

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 icon , the context menu of asset appears:

The screenshot shows the MONARC application interface with the context menu open for the 'Administrator workstations' asset. The menu items are: 1. Edit impacts, 2. Import analysis, 3. Export analysis, 4. See asset in the library, and 5. Detach. The main content area shows a table of 84 information risks for the 'Administrator workstations' asset. The table has columns for Asset, Impact, Threat, Vulnerability, Current risk, Treatment, and Residual risk. Each row contains details about a specific risk, such as 'Forging of rights' or 'Malware infection', along with its associated vulnerabilities and treatment status.

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 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 disabled.

#### 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.

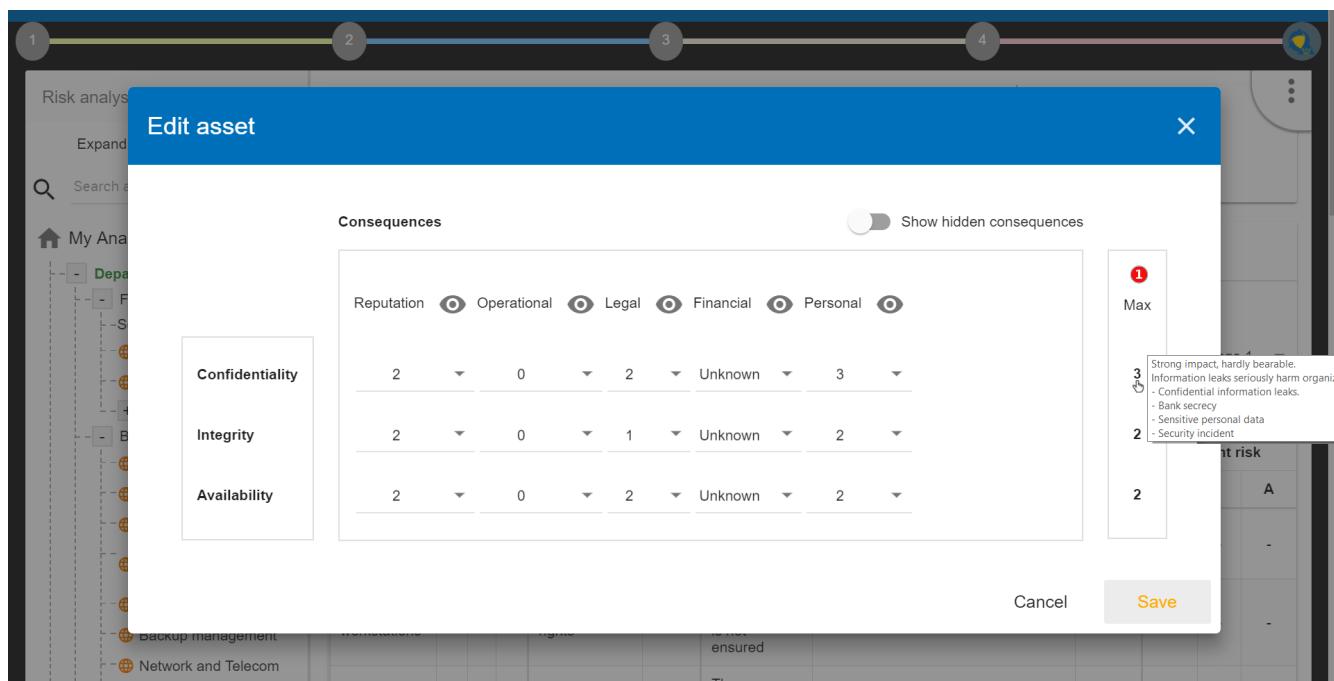


This action may lead to the loss of risk assessments for this asset and its childrens.

### 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.



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. For example, **3** is the consequence of the person in case of disclosure of his personal file.



To hide the consequences that will not consider. Click on the icon . To show it again. Click on [Show hidden consequences](#)

## 4.4. Operational Risks

### 4.4.1. Risks table

The screenshot shows the MONARC software interface for managing operational risks. The top navigation bar includes 'Home > My Analysis' and various settings icons. The left sidebar contains a tree view of assets under 'My Analysis', with 'Department' selected (marked with a red circle). The main area displays the 'Operational risks' tab, which lists '2 operational risks'. The table has columns for Asset, Risk description, Inherent risk (Prob., Impact R, O, L, F, P, Current risk), Net risk (Prob., Impact R, O, L, F, P, Current risk), Existing controls, Treatment (e.g., Not treated), and Target risk. The first risk is 'Prior information to be provided to the person is insufficient' and the second is 'Changes in treatment or further treatment, without prior notification to the data subject'.

1. Select the primary asset. In this case, **Department**.
2. Click on tab **Operational risks**.
3. Total of operational risks associated with primary asset.
4. Ability to select only certain risks, according to the risk acceptance threshold.
5. Ability to sort of most columns of the table.



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](#).

The screenshot shows the 'My Analysis' section of the MONARC interface. At the top, there are four colored status bars: green (labeled 1), blue (labeled 2), orange (labeled 3), and red (labeled 4). Below these are sections for 'Department' (as an entity that regroups persons), 'Confidentiality: 2', 'Integrity: 2', and 'Availability: 2'. A navigation bar at the bottom includes 'Information risks' and 'Operational risks' (which is selected). The main area displays '2 operational risks' for the 'Department' asset. The table has columns for Asset (1), Risk description (2), Inherent risk (3), Net risk (4), Existing controls (5), Treatment (6), and Residual risk (7). The first row shows a risk with a current risk of 12 and a net risk of 6. The second row shows a risk with a current risk of 1 and a net risk of 1. A legend at the top right shows 'Risk threshold (on max NET risk)' with color-coded circles for R (blue), O (green), L (yellow), F (orange), P (red), and Keywords (dark blue). There are also search and download icons.

Asset	Risk description	Inherent risk					Net risk					Treatment	Residual risk			
		Prob.	R	O	L	F	P	Prob.	R	O	L			F	P	
Department	Prior information to be provided to the person is insufficient	3	4	3	2	4	1	12	2	3	2	2	1	6	<a href="#">Not treated</a>	-
Department	Changes in treatment or further treatment, without prior notification to the data subject	-	-	-	-	-	-	-	-	-	-	-	-	<a href="#">Not treated</a>	-	

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 of the ROLFP impact values.
4. **Net risk:** Net risk represents the risk of 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 not yet been treated.

#### 4.4.2. Operational risk sheet

The risk card is displayed when you click on the [Not treated](#) link in the operational risk table.

The screenshot shows the 'Risk sheet' page within the 'My Analysis' section of the MONARC application. The top navigation bar includes 'Home > My Analysis > Risk sheet'. The main content area displays a risk analysis table with the following data:

	Prob.	R	O	L	F	P	MAX risk
Current risk	2	3	2	2	2	1	6
Residual risk	-	-	-	-	-	-	-

Below the table, there are sections for 'Asset' (Department), 'Risk description' (Prior information to be provided to the person is insufficient), 'Risk probability' (2 - Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.), 'Existing controls', 'Recommendations' (with a '+ Add' button), and 'Kind of treatment' (set to 'Not treated'). A 'Save' button is located at the bottom right. The left sidebar contains 'Risk analysis' and 'Assets library' sections, and the bottom left features a search bar for assets.

1. **Back to the list:** Return to risk table.
2. **Current risk:** Values for risk probability (**Prob.**) and ROLFP [2: Reputation, Operational, Legal, Financial and Personal] Criteria.
3. **Residual risk :** Values for risk probability and ROLFP [2: Reputation, Operational, Legal, Financial and Personal] criteria (not yet treated). Those values should be adjusted according to the recommendation and the measures that will be put in place.
4. Reminders of the parameters of the risk table.
5. **Recommendations :** Creation / Assignment button for adding one or more recommendations.
6. **Kind of treatment :** 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



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

The screenshot shows the 'Risk sheet' page for 'My Analysis'. The top navigation bar has four colored dots (green, blue, orange, red) corresponding to the tabs: 'Risk analysis', 'Information risks', 'Operational risks' (which is selected), and 'Residual risk'. The left sidebar includes sections for 'Risk analysis', 'Assets library', and 'My Analysis' (with a 'Department' node selected). The main content area displays a table for 'Operational risks' with columns for Prob., R, O, L, F, P, and MAX risk. A summary table for 'Current risk' and 'Residual risk' is also shown. Below the tables are sections for 'Asset', 'Risk description', 'Risk probability', 'Existing controls', 'Recommendations', and 'Kind of treatment'. A 'Save' button is at the bottom right.

#### 4.4.3. Adding additional risk

When an asset is selected in the analysis:

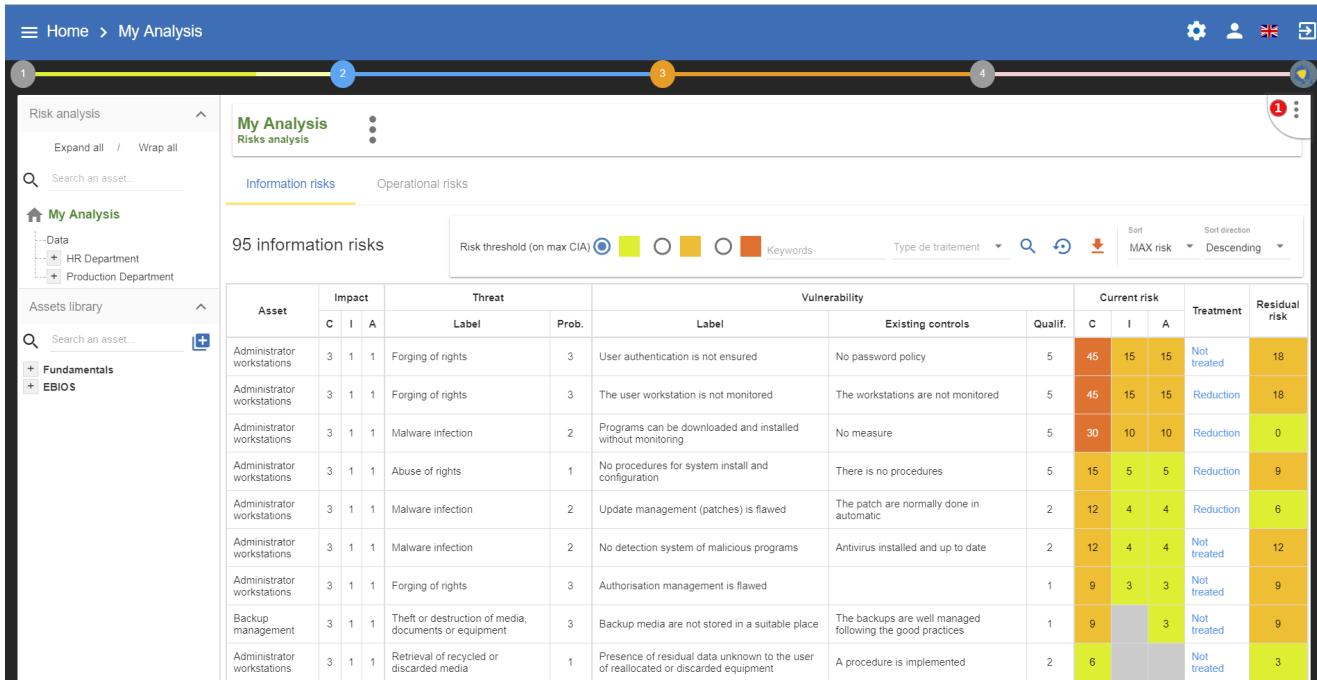
The screenshot shows the 'Risk sheet' page for 'My Analysis' with 'Department' selected in the asset tree. The top navigation bar and sidebar are similar to the previous screenshot. The main content area now displays a table for '2 operational risks' under the 'Department' asset. The table includes columns for Asset, Risk description, Inherent risk (Prob., Impact, Current risk), Net risk (Prob., Impact, Current risk), Existing controls, Treatment, and Residual risk. A 'Create a specific risk' button is at the bottom left. The top right of the screen shows 'Confidentiality: 4', 'Integrity: 3', and 'Availability: 2'.

- 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 right contextual menu



This screenshot shows the MONARC interface with the 'My Analysis' page selected. A contextual menu is open at the top right, indicated by a blue circle with the number '1'. The menu items are: Risk analysis, Risks analysis, Evaluation scales (highlighted in red), Knowledge base, Interviews table, and Snapshots.

**Left sidebar:**

- Risk analysis (selected)
- Expand all / Wrap all
- Search an asset...
- My Analysis**
  - Data
  - + HR Department
  - + Production Department
- Assets library (selected)
- Search an asset...
- + Fundamentals
- + EBIOS

**Top navigation:**

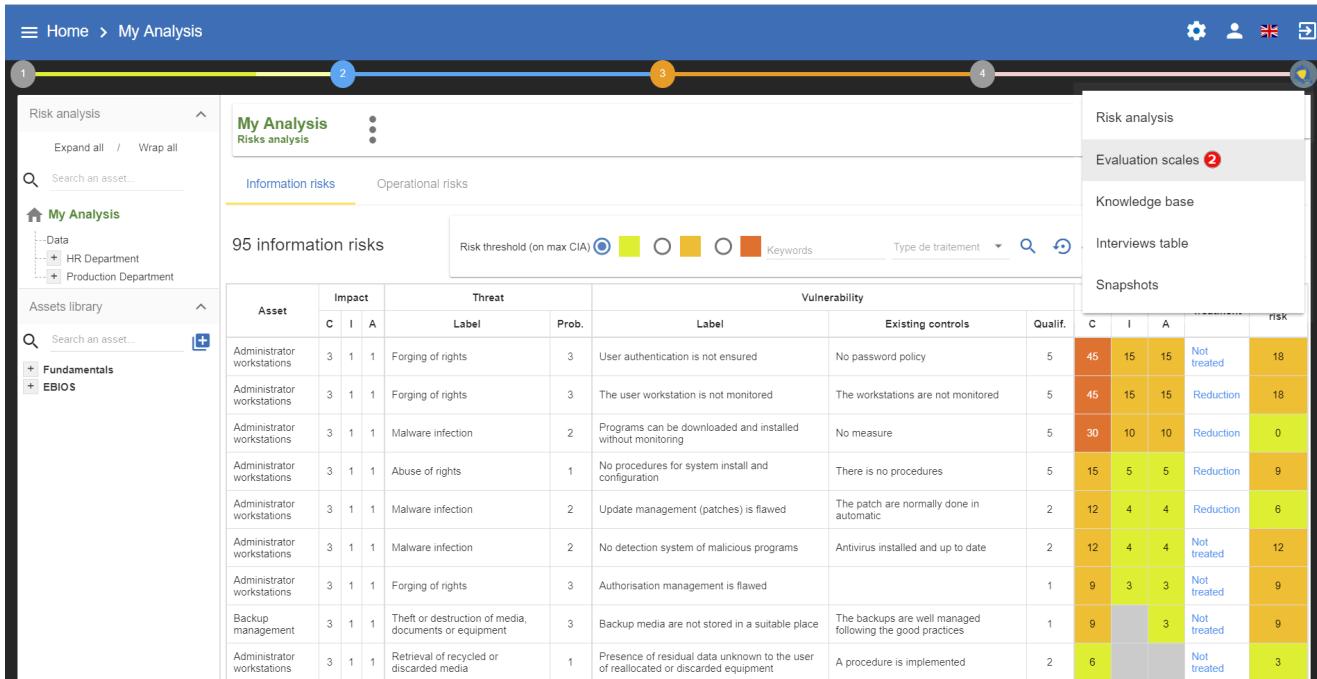
- Home > My Analysis
- Settings icon
- User icon
- UK flag
- Search icon

**Main content:**

95 information risks

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	3	1	1	Forging of rights	3	User authentication is not ensured	No password policy	5	45	15	15	Not treated	18
Administrator workstations	3	1	1	Forging of rights	3	The user workstation is not monitored	The workstations are not monitored	5	45	15	15	Reduction	18
Administrator workstations	3	1	1	Malware infection	2	Programs can be downloaded and installed without monitoring	No measure	5	30	10	10	Reduction	0
Administrator workstations	3	1	1	Abuse of rights	1	No procedures for system install and configuration	There is no procedures	5	15	5	5	Reduction	9
Administrator workstations	3	1	1	Malware infection	2	Update management (patches) is flawed	The patch are normally done in automatic	2	12	4	4	Reduction	6
Administrator workstations	3	1	1	Malware infection	2	No detection system of malicious programs	Antivirus installed and up to date	2	12	4	4	Not treated	12
Administrator workstations	3	1	1	Forging of rights	3	Authorisation management is flawed		1	9	3	3	Not treated	9
Backup management	3	1	1	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place	The backups are well managed following the good practices	1	9		3	Not treated	9
Administrator workstations	3	1	1	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment	A procedure is implemented	2	6			Not treated	3

## 2. Calling the Management view of **Evaluation scales**



This screenshot shows the MONARC interface with the 'My Analysis' page selected. The 'Evaluation scales' view is active, indicated by a red circle with the number '2' on the contextual menu. The menu items are: Risk analysis, Risks analysis, Evaluation scales (highlighted in red), Knowledge base, Interviews table, and Snapshots.

**Left sidebar:**

- Risk analysis (selected)
- Expand all / Wrap all
- Search an asset...
- My Analysis**
  - Data
  - + HR Department
  - + Production Department
- Assets library (selected)
- Search an asset...
- + Fundamentals
- + EBIOS

**Top navigation:**

- Home > My Analysis
- Settings icon
- User icon
- UK flag
- Search icon

**Main content:**

95 information risks

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	3	1	1	Forging of rights	3	User authentication is not ensured	No password policy	5	45	15	15	Not treated	18
Administrator workstations	3	1	1	Forging of rights	3	The user workstation is not monitored	The workstations are not monitored	5	45	15	15	Reduction	18
Administrator workstations	3	1	1	Malware infection	2	Programs can be downloaded and installed without monitoring	No measure	5	30	10	10	Reduction	0
Administrator workstations	3	1	1	Abuse of rights	1	No procedures for system install and configuration	There is no procedures	5	15	5	5	Reduction	9
Administrator workstations	3	1	1	Malware infection	2	Update management (patches) is flawed	The patch are normally done in automatic	2	12	4	4	Reduction	6
Administrator workstations	3	1	1	Malware infection	2	No detection system of malicious programs	Antivirus installed and up to date	2	12	4	4	Not treated	12
Administrator workstations	3	1	1	Forging of rights	3	Authorisation management is flawed		1	9	3	3	Not treated	9
Backup management	3	1	1	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place	The backups are well managed following the good practices	1	9		3	Not treated	9
Administrator workstations	3	1	1	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment	A procedure is implemented	2	6			Not treated	3

The view **Evaluation scales** shows the following criteria:

- Impact scale
- Likelihood scale
- Vulnerability scale

- The management of information risk acceptance thresholds
- 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. Impact scale

Impacts scale: [ 0 - 4 ] <span style="color:red;">1</span>						<span style="color:red;">4</span> New column name	
<input type="checkbox"/> Show hidden impacts <span style="color:red;">2</span>		Confidentiality <span style="color:red;">3</span>	Integrity	Availability	Reputation	Operational	Personal
0	Nonexistent impact. The confidentiality criterion is not important.	Nonexistent impact. The integrity criterion is not important.	Nonexistent impact. The availability criterion is not important.	No consequences	No consequences	No consequences	
1	Weak impact, insignificant. Information leaks are negative to the organization's interests. Example: - Internal information leaks which shouldn't be outside the company: - Memorandum - Internal phone directory	Weak impact, insignificant. Corruption easy to rectify without any consequences. Example: - Internal mail or letter.	Weak impact, insignificant. Unavailability which is inconvenient, but not really harmful for the stakeholders. <span style="color:red;">5</span>	Sporadic media critics	Minor incidents without any impact on customers.	Some inconvenience which will be topped without difficulty (Time waste, procedure reiteration, irritation, etc.).	
2	Average impact, acceptable. Information leaks harm organization's interests. Example: - Moderately sensitive information leaks which are only for a group of people. - Internal networking scheme. - Documentation or source code which is non-critical	Average impact, acceptable. Corruption which brings an inconvenience to the stakeholders. Recovery is easy. Example: - Informational web site.	Average impact, acceptable. Unavailability which brings an inconvenience to the stakeholders. Example: - Maximum time periods consider as unbearable are reached.	Temporary degradation of the company or staff reputation. Occasional media critics	Isolated incidents with a manageable impact on customers.	Significative inconvenience which could be topped with some difficulties (Additional costs, denial of access to commercial delivery, fear, misunderstanding, stress, slight physical ailments, etc.).	
3	Strong impact, hardly bearable. Information leaks seriously harm organization's interest. Example: - Confidential information leaks - Bank secrecy - Sensitive personal data - Security incident	Strong impact, hardly bearable. Corruption which brings a considerable inconvenience to the stakeholders. Example: - Confusion between stakeholders.	Strong impact, hardly bearable. Unavailability which bring a considerable inconvenience to the stakeholders. Example: - Maximum time periods consider as unbearable are reached.	Strong degradation of the company or staff reputation. Serious and repeated media critics.	Interruption of a whole department.	Significative consequences which could be topped, but with some serious difficulties (funds embezzlement, bank ban, deterioration of goods, job loss).	
4	Really strong impact, unbearable. Information leaks almost deadly harm organization's interest. Example: ...	Really strong impact, unbearable. Corruption which can't be recovered.	Really strong impact, unbearable. Unavailability which asks some drastic efforts to recover, or even final	Death of someone. Definitive degradation of the	Complete stop of all services.	Significative consequences almost irremediable, which can't be topped (financial distress, important financial	

1. Click to modify the number of scales.
2. Click on **Show hidden impacts** to show or hide the criteria not used in the analysis.
3. Click on the symbol to hide an unused column.
4. Click on **New column name** to add new impact criteria.
5. Click to edit the headings of each scale.

## 5.2. Likelihood scale

	Leaks which are only for a group of people - Internal networking scheme. - Documentation or source code which is non-critical.	Recovery is easy Example: - Informational web site.	Example Maximum time periods consider as unbearable are not reached.	Occasional media critics	Impact on customers.	Commercial delivery, fear, misunderstanding, stress, slight physical ailments, etc.).
3	Strong impact, hardly bearable. Information leaks seriously harm organization's interest. Example: - Confidential information leaks. - Bank secrecy. - Sensitive personal data - Security incident	Strong impact, hardly bearable. Corruption which brings a considerable inconvenience to the stakeholders. Example: - Confusion between stakeholders.	Strong impact, hardly bearable. Unavailability which bring a considerable inconvenience to the stakeholders. Example: - Maximum time periods consider as unbearable are reached.	Strong degradation of the company or staff reputation. Serious and repeated media critics.	Interruption of a whole department.	Significant consequences which could be topped, but with some serious difficulties (funds embezzlement, bank ban, deterioration of goods, job loss...).
4	Really strong impact, unbearable. Information leaks almost deadly harm organization's interest. Example: - Secret or really sensitive information leaks. - Classified information by the law (the EU, NATO, national...)	Really strong impact, unbearable. Corruption which can't be recovered or bring a permanent downtime.	Really strong impact, unbearable. Unavailability which asks some drastic efforts to recover, or even final. Example: - Important maximum time periods consider as unbearable.	Death of someone. Definitive degradation of the company or staff reputation. International media coverage.	Complete stop of all services	Significant consequences almost irremediable which can't be topped (financial distress, important financial debts, working impossibility, long periods psychological and physiological affection, death, etc.).

Likelihood scale: [ 0 - 4 ] ①

0. Impossible  
1. Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.  
2. Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.  
3. Could happen occasionally.  
4. Very likely: easy to execute, no mentionable investment or knowledge necessary.

Vulnerabilities scale: [ 0 - 5 ]

0. No vulnerabilities.  
1. Very weak vulnerability: Some efficient measures have been already taken, and their effectiveness is controlled.  
Very high maturity: Good practices are implemented and frequently verified.  
2. Weak vulnerability: Some efficient measures have been already taken.  
High maturity: Good practices are implemented.  
3. Average vulnerability: Some measures have been already taken, even though they could be better.  
Average maturity: Good practices are implemented without searching a better way.  
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.  
5. Very strong vulnerability: No measures have been implemented.  
Very low maturity or no maturity at all.

Acceptance thresholds of information risks

TxV



## 1. Click to modify the number of scales

## 2. Click to edit the heading on each scale (Management identical to the impact scale).

## 5.3. Vulnerability scale

Likelihood scale: [ 0 - 4 ]

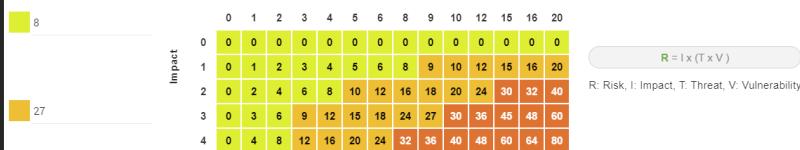
0. Impossible  
1. Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.  
2. Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.  
3. Could happen occasionally.  
4. Very likely: easy to execute, no mentionable investment or knowledge necessary.

Vulnerabilities scale: [ 0 - 5 ] ①

0. No vulnerabilities.  
1. Very weak vulnerability: Some efficient measures have been already taken, and their effectiveness is controlled.  
Very high maturity: Good practices are implemented and frequently verified.  
2. Weak vulnerability: Some efficient measures have been already taken.  
High maturity: Good practices are implemented.  
3. Average vulnerability: Some measures have been already taken, even though they could be better.  
Average maturity: Good practices are implemented without searching a better way.  
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.  
5. Very strong vulnerability: No measures have been implemented.  
Very low maturity or no maturity at all.

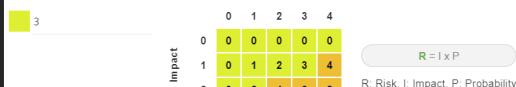
Acceptance thresholds of information risks

TxV



Acceptance thresholds of operational risks

Probability



## 1. Click to modify the number of scales

## 2. Click to edit the heading on each scale (Management identical to the impact scale).

## 5.4. Acceptance thresholds

There are two separate tables for acceptability thresholds, as operational risk and information risk are not calculated in the same way. Information risks are calculated using three criteria:

1. Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.
2. Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.
3. Could happen occasionally.
4. Very likely: easy to execute, no mentionable investment or knowledge necessary.

Vulnerabilities scale: [ 0 - 8 ]

- 0: No vulnerabilities
- 1: Very weak vulnerability. Some efficient measures have been already taken, and their effectiveness is controlled.
- 2: Very high maturity. Good practices are implemented and frequently verified.
- 3: Weak vulnerability. Some efficient measures have been already taken.
- 4: High maturity. Good practices are implemented.
- 5: Average vulnerability. Some measures have been already taken, even though they could be better.
- 6: Average maturity. Good practices are implemented without searching a better way.
- 7: Strong vulnerability. Some measures have been already taken, even though they are ineffective or unadapted.
- 8: Low maturity. Good practices aren't implemented, but there are some positive reactions without any thoughts.
- 9: Very strong vulnerability. No measures have been implemented.
- 10: Very low maturity or no maturity at all.

Acceptance thresholds of information risks

		TxV																		
		0	1	2	3	4	5	6	8	9	10	12	15	16	20					
Impact	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	1	2	3	4	5	6	8	9	10	12	15	16	20					
Impact	2	0	2	4	6	8	10	12	16	18	20	24	30	32	40					
	3	0	3	6	9	12	15	18	24	27	30	36	45	48	60					
Impact	4	0	4	8	12	16	20	24	32	36	40	48	60	64	80					

$$R = I \times (T \times V)$$

R: Risk, I: Impact, T: Threat, V: Vulnerability

Acceptance thresholds of operational risks

		Probability				
		0	1	2	3	4
Impact	0	0	0	0	0	0
	1	0	1	2	3	4
Impact	2	0	2	4	6	8
	3	0	3	6	9	12
Impact	4	0	4	8	12	16

$$R = I \times P$$

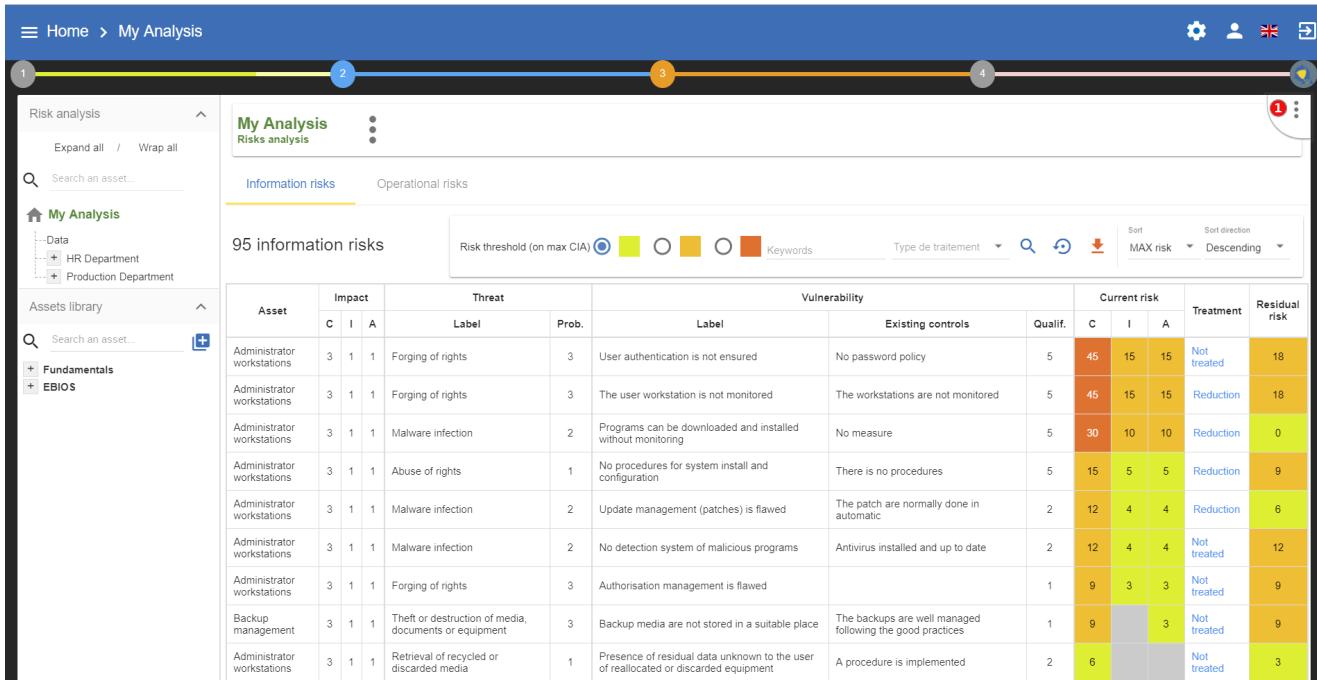
R: Risk, I: Impact, P: Probability

1. Modification of threshold levels of information risks. The table displayed above (as well as the risk analysis tables) is updated automatically.
2. Information risks are calculated using three criteria: **Impact x Threat x Vulnerability**
3. Modification of threshold levels of operational risks. The table displayed above (as well as the risk analysis tables) is updated automatically.
4. Operational risks are calculated using two criteria: **Impact x Probability**

# 6. Management of Knowledge Base

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

1. Calling the right contextual menu 



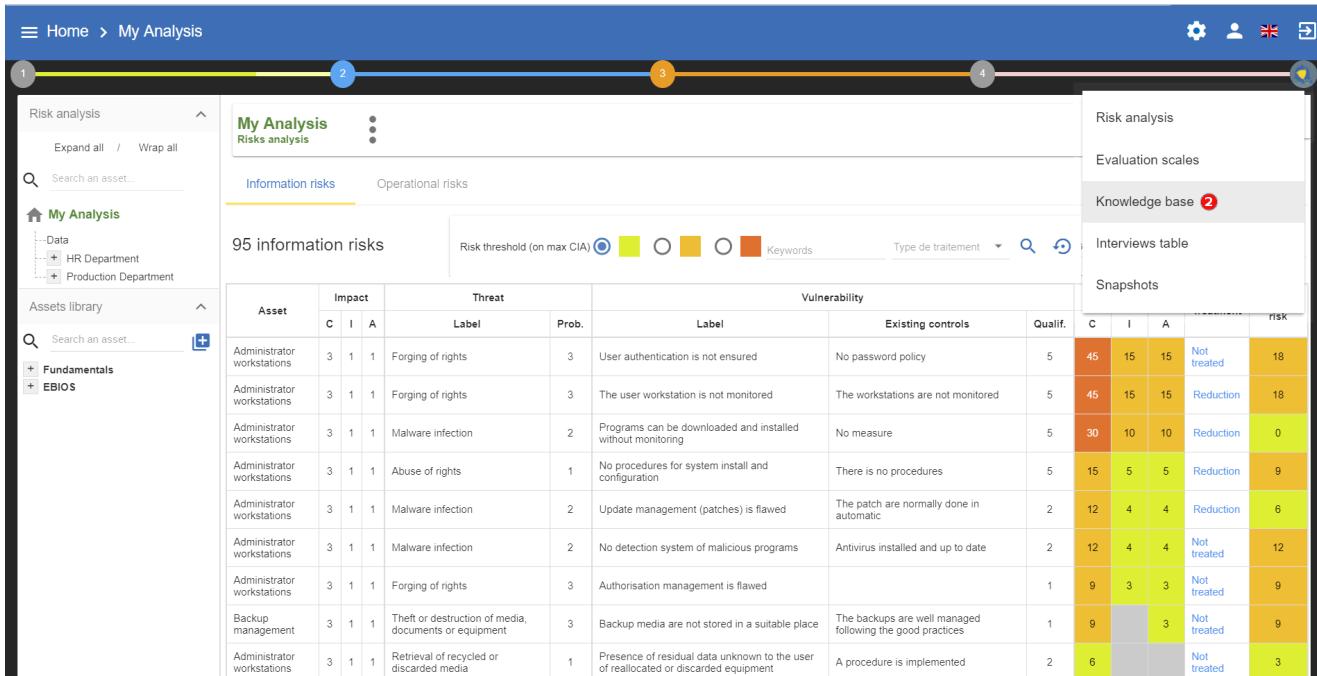
**My Analysis Risks analysis**

Information risks Operational risks

95 information risks

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	3	1	1	Forging of rights	3	User authentication is not ensured	No password policy	5	45	15	15	Not treated	18
Administrator workstations	3	1	1	Forging of rights	3	The user workstation is not monitored	The workstations are not monitored	5	45	15	15	Reduction	18
Administrator workstations	3	1	1	Malware infection	2	Programs can be downloaded and installed without monitoring	No measure	5	30	10	10	Reduction	0
Administrator workstations	3	1	1	Abuse of rights	1	No procedures for system install and configuration	There is no procedures	5	15	5	5	Reduction	9
Administrator workstations	3	1	1	Malware infection	2	Update management (patches) is flawed	The patch are normally done in automatic	2	12	4	4	Reduction	6
Administrator workstations	3	1	1	Malware infection	2	No detection system of malicious programs	Antivirus installed and up to date	2	12	4	4	Not treated	12
Administrator workstations	3	1	1	Forging of rights	3	Authorisation management is flawed		1	9	3	3	Not treated	9
Backup management	3	1	1	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place	The backups are well managed following the good practices	1	9		3	Not treated	9
Administrator workstations	3	1	1	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment	A procedure is implemented	2	6			Not treated	3

2. Calling the Management view of Knowledge base



**My Analysis Risks analysis**

Information risks Operational risks

95 information risks

Asset	Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	3	1	1	Forging of rights	3	User authentication is not ensured	No password policy	5	45	15	15	Not treated	18
Administrator workstations	3	1	1	Forging of rights	3	The user workstation is not monitored	The workstations are not monitored	5	45	15	15	Reduction	18
Administrator workstations	3	1	1	Malware infection	2	Programs can be downloaded and installed without monitoring	No measure	5	30	10	10	Reduction	0
Administrator workstations	3	1	1	Abuse of rights	1	No procedures for system install and configuration	There is no procedures	5	15	5	5	Reduction	9
Administrator workstations	3	1	1	Malware infection	2	Update management (patches) is flawed	The patch are normally done in automatic	2	12	4	4	Reduction	6
Administrator workstations	3	1	1	Malware infection	2	No detection system of malicious programs	Antivirus installed and up to date	2	12	4	4	Not treated	12
Administrator workstations	3	1	1	Forging of rights	3	Authorisation management is flawed		1	9	3	3	Not treated	9
Backup management	3	1	1	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place	The backups are well managed following the good practices	1	9		3	Not treated	9
Administrator workstations	3	1	1	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment	A procedure is implemented	2	6			Not treated	3

All parameters are managed with the same view:

Status	Label	Code	Type	Description	Actions
<input type="checkbox"/>	✓ Company directory	SYS_ANU	Secondary	Company directory	
<input type="checkbox"/>	✓ Business application	LOG_APP	Secondary	Custom business application or standard	
<input type="checkbox"/>	✓ Other media	MAT_NELE	Secondary	Paper, slide, transparency, documentation, fax.	
<input type="checkbox"/>	✓ Backup	OV_BACKUP	Secondary	Backup	
<input type="checkbox"/>	✓ Building, office or premises	OV_BATI	Secondary	Building, office or premises	
<input type="checkbox"/>	✓ Container	CONT	Primary	Asset container	
<input type="checkbox"/>	✓ Decision maker	PER_DEC	Secondary	Decision maker	
<input type="checkbox"/>	✓ Software development	OV_DEVELOPPEMENT	Secondary	Software development	
<input type="checkbox"/>	✓ Developer	PER_DEV	Secondary	Developer	
<input type="checkbox"/>	✓ Internet access device	SYS_INT	Secondary	Internet access device	
<input type="checkbox"/>	✓ Paper document	OV_INFOPHY	Secondary	Information in physical form	
<input type="checkbox"/>	✓ Operator / Maintenance	PER_EXP	Secondary	Operator / Maintenance	

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 (e.g. 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. Vulnerabilities

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 right contextual menu

This screenshot shows the MONARC interface with a contextual menu open at the top right. The menu items are: Risk analysis, Evaluation scales, Knowledge base, Interviews table (with a red notification badge), and Snapshots. The main dashboard displays a table of 95 information risks, categorized by threat and vulnerability, with columns for Impact (C, I, A), Threat (Label, Prob.), Vulnerability (Label, Existing controls, Qualif.), Current risk (C, I, A), Treatment, and Residual risk. The table includes rows for various assets like administrator workstations, backup management, and EBIOS, detailing specific risks such as 'Forging of rights' and 'Malware infection'.

## 2. Calling the Management view of Interviews

This screenshot shows the MONARC interface with the 'Interviews table' option selected from the contextual menu. The main dashboard displays the same table of 95 information risks as in the previous screenshot. The contextual menu is now closed, and the 'Interviews table' option is highlighted. The table structure remains the same, showing the detailed analysis for each asset across various threat and vulnerability categories.

Interviews table			
Add an interview			
Date	Department / People	Contents	Actions
3 1 1	Malware infection	2	Update management (patches) is flawed The patch are normally done in automatic
3 1 1	Malware infection	2	No detection system of malicious programs Antivirus installed and up to date
3 1 1	Forging of rights	3	Authorisation management is flawed
Backup management	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place The backups are well managed following the good practices
Administrator workstations	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment A procedure is implemented

## 1. Click to encode a new interview

Interviews table			
Add an interview			
Date (July 10, 2015; Week 3; First month...)	Department / People	Contents	Actions
3 1 1	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place The backups are well managed following the good practices
Administrator workstations	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment A procedure is implemented

Some information has to be entered

1. Date
2. Names of people or name of the department
3. The subjects covered.
4. Once all the fields are filled, create an interview

# 8. Snapshots

Snapshots allow you to create a full backup for 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 to the changes.

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

## 1. Calling the right contextual menu

This screenshot shows the MONARC interface with the 'My Analysis' section selected. The top navigation bar has four numbered circles (1, 2, 3, 4) corresponding to the UI elements shown in the callout. The main content area displays a table of 95 information risks, categorized by threat and vulnerability, with various status indicators and risk scores.

Asset	Impact			Threat			Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A			
Administrator workstations	3	1	1	Forging of rights	3	User authentication is not ensured	No password policy	5	45	15	15	Not treated	18	
Administrator workstations	3	1	1	Forging of rights	3	The user workstation is not monitored	The workstations are not monitored	5	45	15	15	Reduction	18	
Administrator workstations	3	1	1	Malware infection	2	Programs can be downloaded and installed without monitoring	No measure	5	30	10	10	Reduction	0	
Administrator workstations	3	1	1	Abuse of rights	1	No procedures for system install and configuration	There is no procedures	5	15	5	5	Reduction	9	
Administrator workstations	3	1	1	Malware infection	2	Update management (patches) is flawed	The patch are normally done in automatic	2	12	4	4	Reduction	6	
Administrator workstations	3	1	1	Malware infection	2	No detection system of malicious programs	Antivirus installed and up to date	2	12	4	4	Not treated	12	
Administrator workstations	3	1	1	Forging of rights	3	Authorisation management is flawed		1	9	3	3	Not treated	9	
Backup management	3	1	1	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place	The backups are well managed following the good practices	1	9		3	Not treated	9	
Administrator workstations	3	1	1	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment	A procedure is implemented	2	6			Not treated	3	

## 2. Calling the Management view of Snapshot

This screenshot shows the MONARC interface with the 'My Analysis' section selected. The top navigation bar has four numbered circles (1, 2, 3, 4) corresponding to the UI elements shown in the callout. The main content area displays a table of 95 information risks, similar to the first screenshot, but with a different set of filters and sorting applied. A vertical sidebar on the right lists various management functions, with 'Snapshots' highlighted.

The following pop-up appears:

The screenshot shows the MONARC interface with a focus on the 'Snapshots' feature. A modal window titled 'Add a snapshot' is open, prompting the user to enter an optional comment ('First snapshot') and create a new snapshot. Below this, a table lists existing snapshots, including the current one ('First snapshot'). The main dashboard displays a risk analysis report with sections for 'Information risks' and 'Operational risks', and includes a search bar and navigation menu.

1. **Create** a Snapshot: Possibility to enter a comment allowing to contextualize the snapshot. There are some possible actions:
2. **View** a Snapshot
3. **Restore** Snapshot. Caution this option will overwrite the current analysis.
4. **Delete** a Snapshot.

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

The screenshot shows the MONARC interface in snapshot mode. A blue header bar at the top indicates that changes cannot be made. To the right, a button allows returning to the risk analysis. The main content area displays a risk analysis report for '[SNAP] My Analysis' with a table of 95 information risks. The table includes columns for Asset, Impact, Threat, Vulnerability, Current risk, Treatment, and Residual risk. The rows list various findings such as 'Forging of rights', 'Malware infection', and 'Abuse of rights' across different workstation types.

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

# 9. Managing the Implementation Treatment Plan

By clicking on the number 4, the following menu will appear:

The screenshot shows the MONARC user interface with a navigation bar at the top. The main content area displays a table of 84 information risks. A callout box highlights the 'Management of the implementation of the risk treatment plan' option under the 'Implementation and monitoring' section.

Asset	Impact	Threat	Vulnerability			Qualif.	Current risk			Treatment	Residual risk	
C	I	A	Label	Prob.	Label		C	I	A			
Administrator workstations	3	1	Forging of rights	3	The user workstation is not monitored	The workstations are not monitored	5	45	15	15	Reduction	18
Administrator workstations	3	1	Forging of rights	3	Authorisation management is flawed	No procedure	4	36	12	12	Reduction	9
Administrator workstations	3	1	Malware infection	2	Programs can be downloaded and installed without monitoring	No measure	5	30	10	10	Reduction	0
Administrator workstations	3	1	Abuse of rights	1	No procedures for system install and configuration	There is no procedures	5	15	5	5	Not treated	15
Administrator workstations	3	1	Malware infection	2	Update management (patches) is flawed	The patch are normally done in automatic	2	12	4	4	Not treated	12
Administrator workstations	3	1	Malware infection	2	No detection system of malicious programs	Antivirus installed and up to date	2	12	4	4	Not treated	12
Administrator workstations	3	1	Forging of rights	3	User authentication is not ensured	No password policy	1	9	3	3	Not treated	9
Backup management	3	1	Theft or destruction of media, documents or equipment	3	Backup media are not stored in a suitable place	The backups are well managed following the good practices	1	9		3	Not treated	9
Administrator workstations	3	1	Retrieval of recycled or discarded media	1	Presence of residual data unknown to the user of reallocated or discarded equipment	A procedure is implemented	2	6			Not treated	6

This view goes beyond the ISO/IEC 27005, as it enables the user to manage the follow-up to the implementation of the measures.

The screenshot shows the MONARC user interface with a navigation bar at the top. The main content area displays a table of recommendations for the implementation of the risk treatment plan. A callout box highlights the 'Open the implementation history' button.

Recommendation	Imp.	Comment	Manager	Deadline	Status	Actions
Authorisation Implement a procedure for the authorisation management	***			jj-mm-yyyy	Coming	<a href="#">Edit</a>
Monitoring Implement e a monitoring of the workstation	***			jj-mm-yyyy	Coming	<a href="#">Edit</a>
Program management Implement a white list of the program which have been approved by the IT department	***			jj-mm-yyyy	Coming	<a href="#">Edit</a>
Administrator right Remove the administrator right from the workstations of the users	**			jj-mm-yyyy	Coming	<a href="#">Edit</a>
Patch management Check if the patch are really applied	**			jj-mm-yyyy	Coming	<a href="#">Edit</a>

1. This is a **recommendation** established before.
2. You can put a **comment** for the implementation of the recommendation.
3. For each recommendation you can set a **manager**.
4. For each recommendation you can set a **deadline**.

## 5. Status of Implementation.

6. Click on the icon  to implement the recommendation and switch on the following view.

Asset	Threat	Vulnerability	Existing controls	Current risk	New controls	Residual risk	Actions
Administrator workstations	MD14 - Forging of rights	1166 - Authorisation management is flawed	No procedure	38	1	9	

1. Set the **new control**, now in place. It will replace the old one in the risk analysis and replace the old current risk by the residual risk.

2. Launches the pop-up validation of the update below by clicking on the icon 

Follow the same procedure for each recommendation. After that go to your risk analysis and make a second iteration.

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

All validations are stored in history and can be consulted:

	Recommendation	Imp.	Comment	Manager	Deadline	Status	Actions
	Monitoring Implement e a monitoring of the workstation	***			jj-mm-yyyy	Coming	
	Program management Implement a white list of the program which have been approved by the IT department	***			jj-mm-yyyy	Coming	
	Administrator right Remove the administrator right from the workstations of the users	**			jj-mm-yyyy	Coming	
	Patch management Check if the patch are really applied	**			jj-mm-yyyy	Coming	

## 1. Click to view past recommendations

By	Recommendation	Risk	Implementation comment	Risk before	Risk after
Jérôme Lombardi	<b>*** Authorisation</b> Implement a procedure for the authorisation management Comment: Deadline: Manager:	<b>Asset type:</b> OV_POSTE_FIXE - Ordinateur de bureau <b>Asset:</b> Postes de travail admin <b>Threat:</b> MD14 - Utilisation de droits <b>Vulnerability:</b> 1166 - La gestion des autorisations comporte des failles <b>Treatment type:</b> Reduction <b>Existing controls:</b> No procedure <b>New controls:</b>		36	9