



OPTIMISED RISK ANALYSIS

www.monarc.lu

User Guide

CASES Luxembourg

Version 2019-10-04

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. Home page	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	33
5.1. Impact scale	34
5.2. Likelihood scale	34
5.3. Vulnerability scale	35
5.4. Acceptance thresholds	35
6. Management of Knowledge Base	37
6.1. Type of assets	39
6.2. Threats	39
6.3. Vulnerabilities	39
6.4. Referentials	40
6.5. Risks	40
6.6. Tags (Operational Risks)	41
6.7. Operational Risks	42
6.8. Recommendations Sets	42
7. Statement of applicability	43
8. Dashboard	46
9. Record of processing activities	48
9.1. Description	50
9.2. Actors	51
9.3. Categories of data subjects and personal data	52
9.4. Recipients	52
9.5. International transfers	53

9.6. Processors	54
10. Interviews	55
11. Snapshots	57
12. Managing the Implementation Treatment Plan	59

Chapter 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.

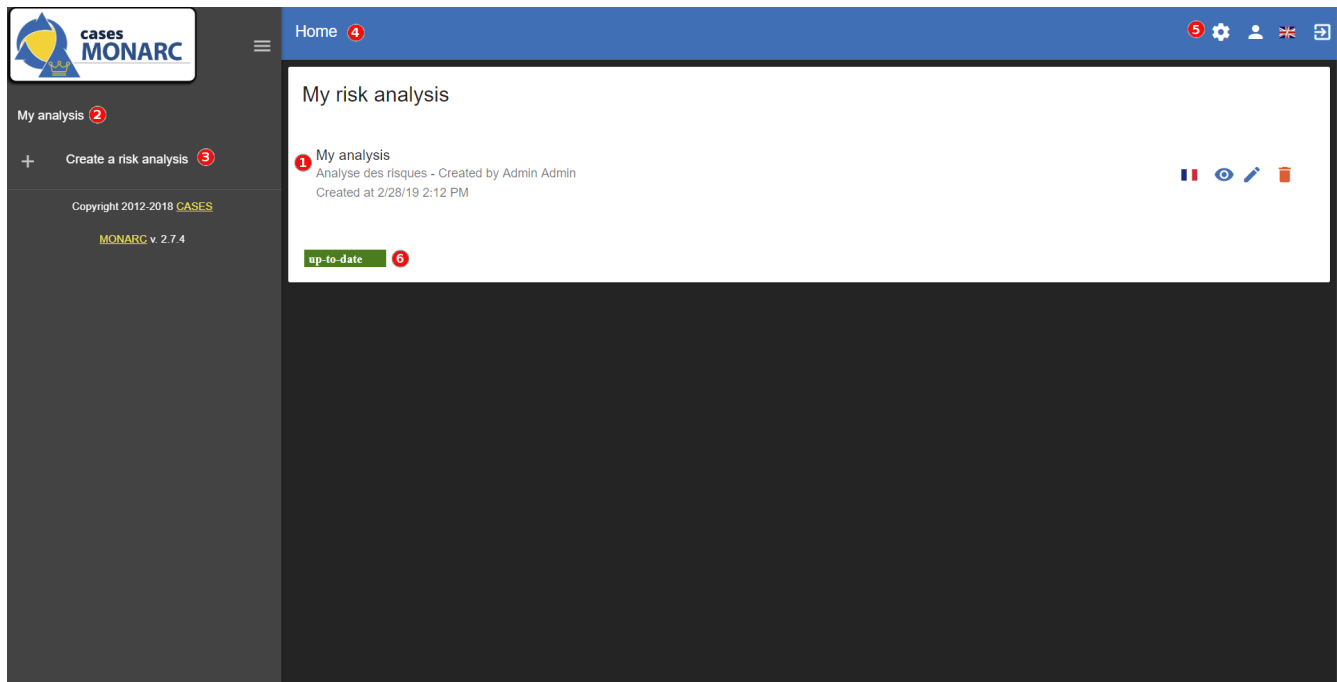


Export any table (.csv) or graphic (.png).

Chapter 2. Home Page

2.1. Home page

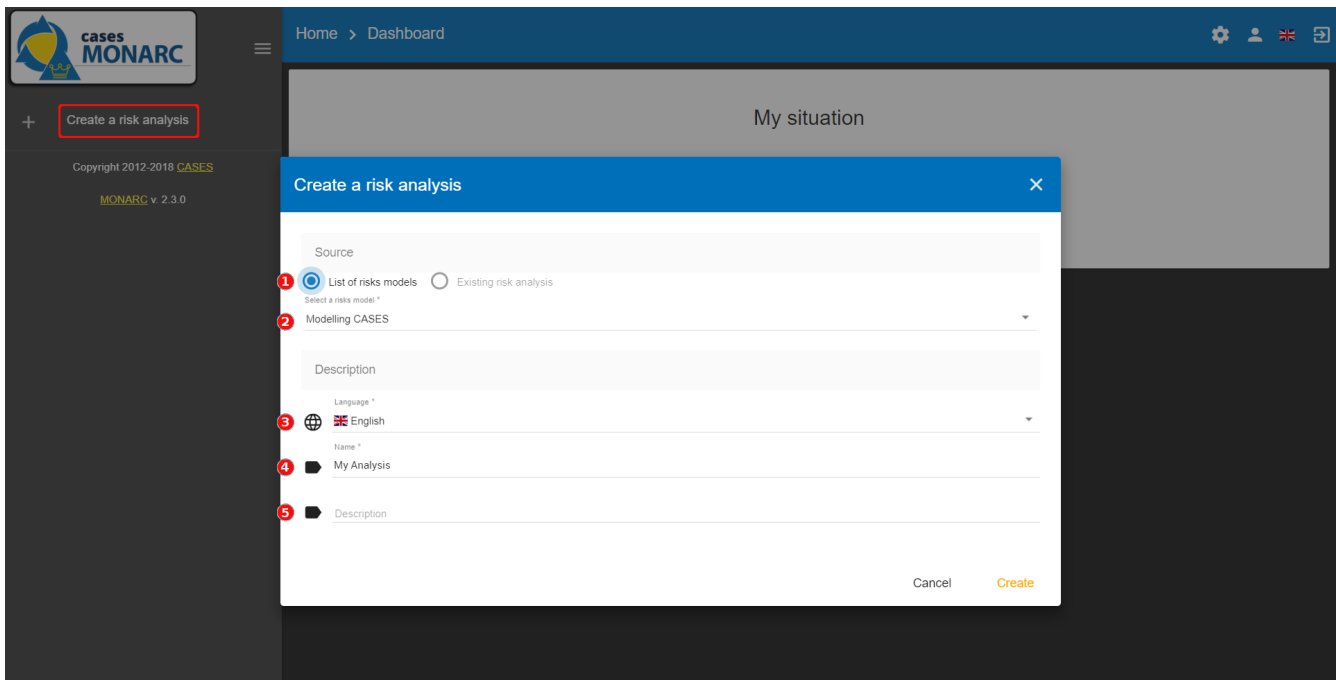
Immediately after user authentication, the following screen appears. It may, however, be slightly different, if there is not yet an analysis created or if there are already several and according to the state of progress of the analysis.



1. Graph showing the statistics of the last modified 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](#)).
6. Inform you if an update of MONARC is available.

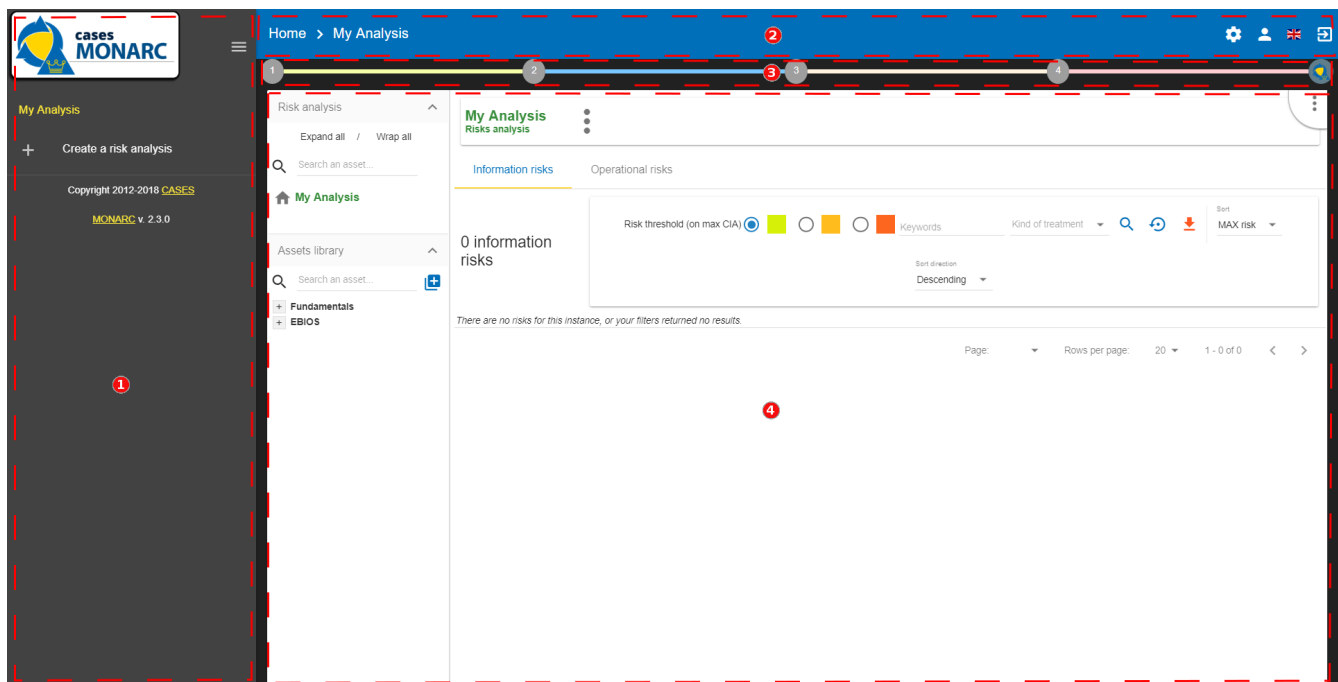
2.2. Creating a Risk Analysis

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 left column 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.

Chapter 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

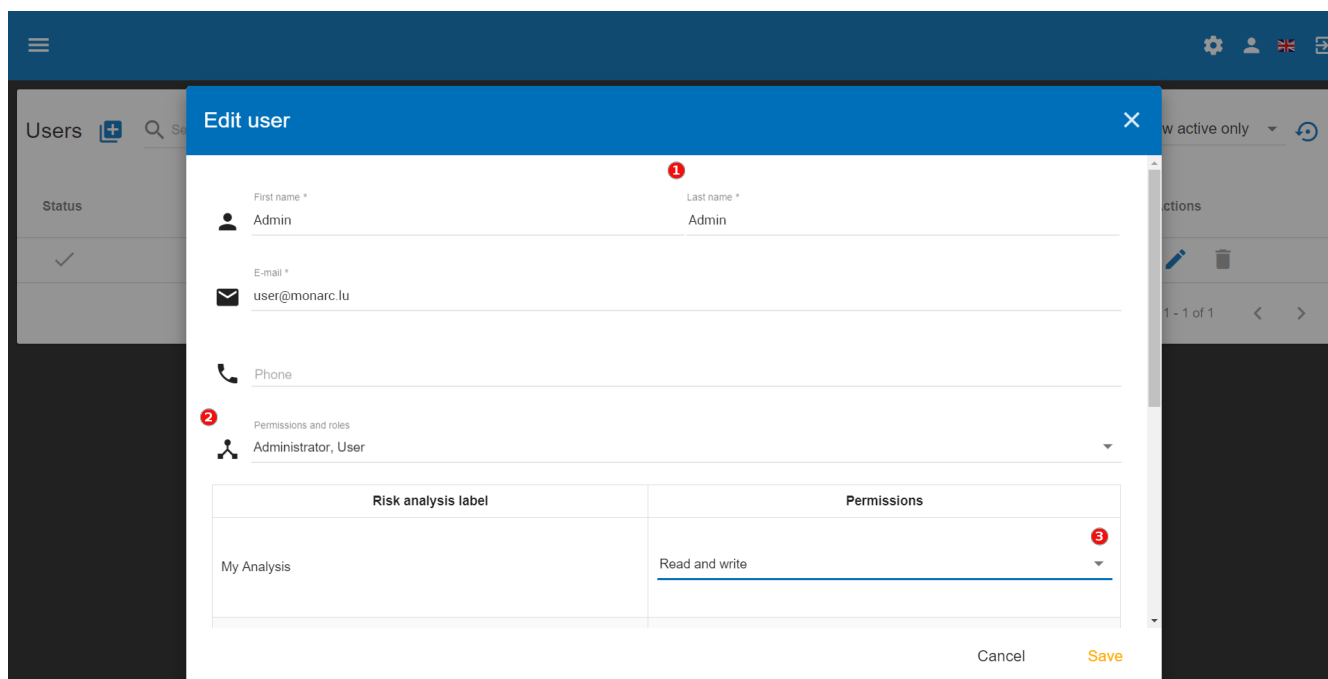
List of users

Home > Administration > Users					
Users 1 + <input type="text" value="Search..."/>					
Status 2	First name ↓	Last name 3	E-mail	Phone	Actions 4 5
✓	Admin	Admin	user@monarc.lu		4 5
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.

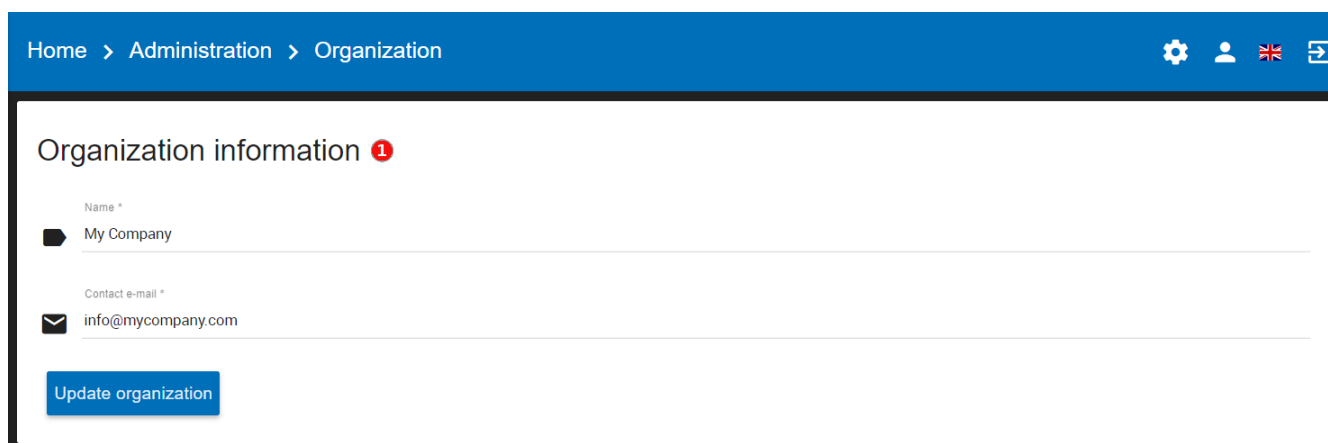
User rights and information

After clicking on the icon , the following screen appears:



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



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.

Deliverable templates					
Deliverable template for context validation					
Description	French	English	German	Dutch	Actions
Context validation	✓	✓	✓	✓	Download
My Personal template		✓			Download Edit Delete
Deliverable template for model validation					
Description	French	English	German	Dutch	Actions
Modelling validation	✓	✓	✓	✓	Download
Deliverable template for final report					
Description	French	English	German	Dutch	Actions
Report risk assessment	✓	✓	✓	✓	Download
Deliverable template for Implementation plan					
Description	French	English	German	Dutch	Actions
Implementation plan	✓	✓	✓	✓	Download

This view summarize 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 :

Deliverable templates					
Deliverable template for context validation					
Description					Actions
Context validation					Download
My Personal template					Download Edit Delete
Deliverable template for model validation					
Description					Actions
Modelling validation					Download
Deliverable template for final report					
Description					Actions
Report risk assessment					Download
Deliverable template for Implementation plan					
Description					Actions
Implementation plan					Download

Add a deliverable template

Category *

Language

Description

French

English

German

Dutch

Drop your DOCX file in this zone, or click here to select a file

Drop your DOCX file in this zone, or click here to select a file

Drop your DOCX file in this zone, or click here to select a file

Drop your DOCX file in this zone, or click here to select a file

Drop your DOCX file in this zone, or click here to select a file

Cancel Create

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	30	Reduction	6
20		30	Reduction	6
18	18	24	Reduction	0
18		24	Reduction	0
16	16	24	Reduction	18
4	16	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 interface. On the left, a sidebar titled 'Context Establishment' lists four steps: 1. Risks analysis context, 2. Evaluation of Trends and Threat, and synthesis, 3. Risks management organisation, and 4. Definition of the risk evaluation criteria. The main area displays a risk assessment table for 'Information risks'.

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Existing controls	C		I	A			
Postes de travail utilisateur	2	2	3	Usurpation de droits	3	La gestion des autorisations comporte des failles	Contrôle d'accès inexistant	5	30	30	45	Not treated	45	
Gestion des backups	2	2	3	Dysfonctionnement ou panne du matériel	2	Les backups ne sont pas réalisés selon l'état de l'art	Les backups sont réalisés sur cassettes toutes les nuits. Les cassettes sont changées chaque jour et conservées 7 jours. Une cassette est réservée chaque mois pendant 1 an. Aucun test de restauration n'est effectué.	5		20	30	Reduction	6	
Gestion des backups	2	2	3	Vol ou destruction de supports, de documents ou de matériel	2	Les supports de backup ne sont pas entreposés dans un endroit adéquat	Les Backups ne sont pas chiffrés. Les cassettes sont entreposées dans une armoire non verrouillée, parce que plusieurs services y ont accès.	5	20		30	Reduction	6	
Administrateur IT	3	3	4	Erreur d'utilisation	2	Absence de charte informatique précisant les exigences d'utilisation	Pas de charte, ni consigne d'utilisation du système d'information.	3	18	18	24	Reduction	0	
Bâtiment	3	3	4	Vol ou destruction de supports, de documents ou de matériel	2	Le principe du moindre privilège n'est pas appliqué	Pas de contrôle d'accès	3	18		24	Reduction	0	
Organisation informatique	2	2	3	Usurpation de droits	2	Absence de contrôle périodique des autorisations d'accès logique	La revue de droit sur l'Active Directory est faite, mais n'est pas optimale.	4	16	16	24	Reduction	18	
Organisation informatique	2	2	3	Vol ou destruction de supports, de documents ou de matériel	2	Absence de contrôle périodique des autorisations d'accès physique		4	16		24	Not treated	24	

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:

Context modeling

- ☒ Identification of assets, vulnerabilities and impacts appreciation
- ☒ Synthesis of assets / impacts **1**

Deliverable: Model validation

138 information risks

Asset	Impact			Threat		Vulnerability	Qualif.	Current risk			Treatment	Residual risk
	C	I	A	Label	Prob.			C	I	A		
Postes de travail utilisateur	2	2	3	Usurpation de droits	3	La gestion des autorisations comporte des failles	5	30	30	45	Not treated	45
Gestion des backups	2	2	3	Dysfonctionnement ou panne du matériel	2	Les backups ne sont pas réalisés selon l'état de l'art	5		20	30	Reduction	6
Gestion des backups	2	2	3	Vol ou destruction de supports, de documents ou de matériel	2	Les supports de backup ne sont pas entreposés dans un endroit adéquat	5	20		30	Reduction	6
Administrateur IT	3	3	4	Erreur d'utilisation	2	Absence de charte informatique précisant les exigences d'utilisation	3	18	18	24	Reduction	0
Bâtiment	3	3	4	Vol ou destruction de supports, de documents ou de matériel	2	Le principe du moindre privilège n'est pas appliqué	3	18		24	Reduction	0
Organisation informatique	2	2	3	Usurpation de droits	2	Absence de contrôle périodique des autorisations d'accès logique	4	16	16	24	Reduction	18
Organisation informatique	2	2	3	Vol ou destruction de supports, de documents ou de matériel	2	Absence de contrôle périodique des autorisations d'accès physique	4	16		24	Not treated	24

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:

Deliverable

Status: Draft

Template: Rapport final

Version: 1.0

Classification: TLP: RED

Document name: Final document

Client manager(s): Client

Security consultant(s): CASES

Summary of risk evaluation:

Management summary

1

Cancel Save

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:

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 modify).

Chapter 4. Analysis Management

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

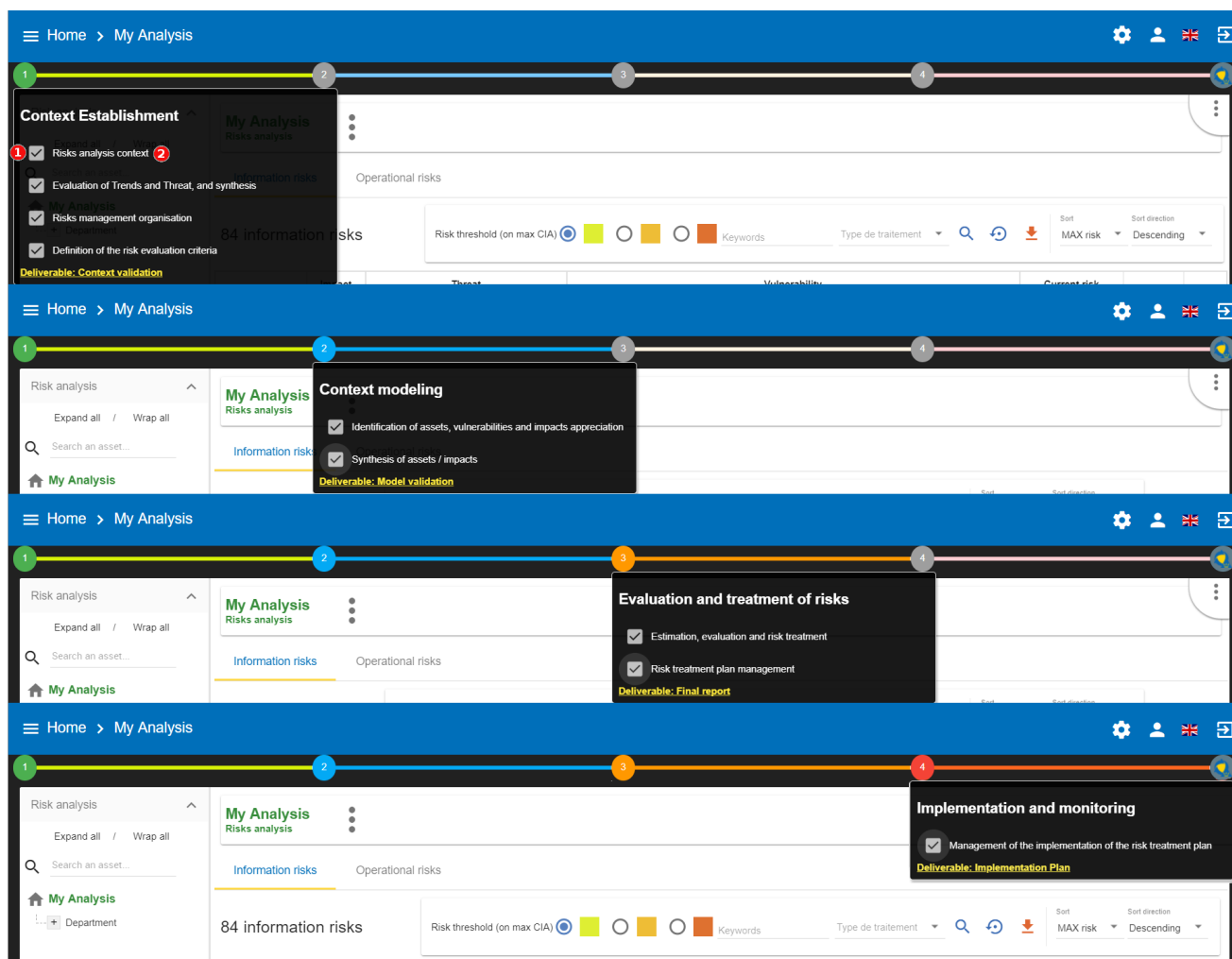
The screenshot displays the MONARC Risk Analysis interface. It features a top navigation bar (1) with 'Home' and 'My Analysis' links. On the left, there is an 'Assets library' sidebar (2) with a search bar and a list of assets. The main area is divided into a 'Risk analysis' sidebar (3) with 'Expand all' and 'Wrap all' options, and a main table area (4) showing '84 information risks'. The table has columns for Asset, Impact, Threat, Vulnerability, Current risk, and Treatment. The table data is as follows:

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 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 Risk Analysis interface. On the left, the 'Assets library' sidebar contains a search bar (1) and a tree view of categories (3). The tree view includes 'Fundamentals' (4) and 'EBIOS' (5). The main area displays '84 information risks' in a table. The table has columns for Asset, Impact (C, I, A), Threat (Label, Prob.), Vulnerability (Label, Existing controls, Qualif.), Current risk (C, I, A), Treatment, and Target risk. The table lists several rows of risks, such as 'Forging of rights' and 'Malware infection', with their respective assets and treatments.

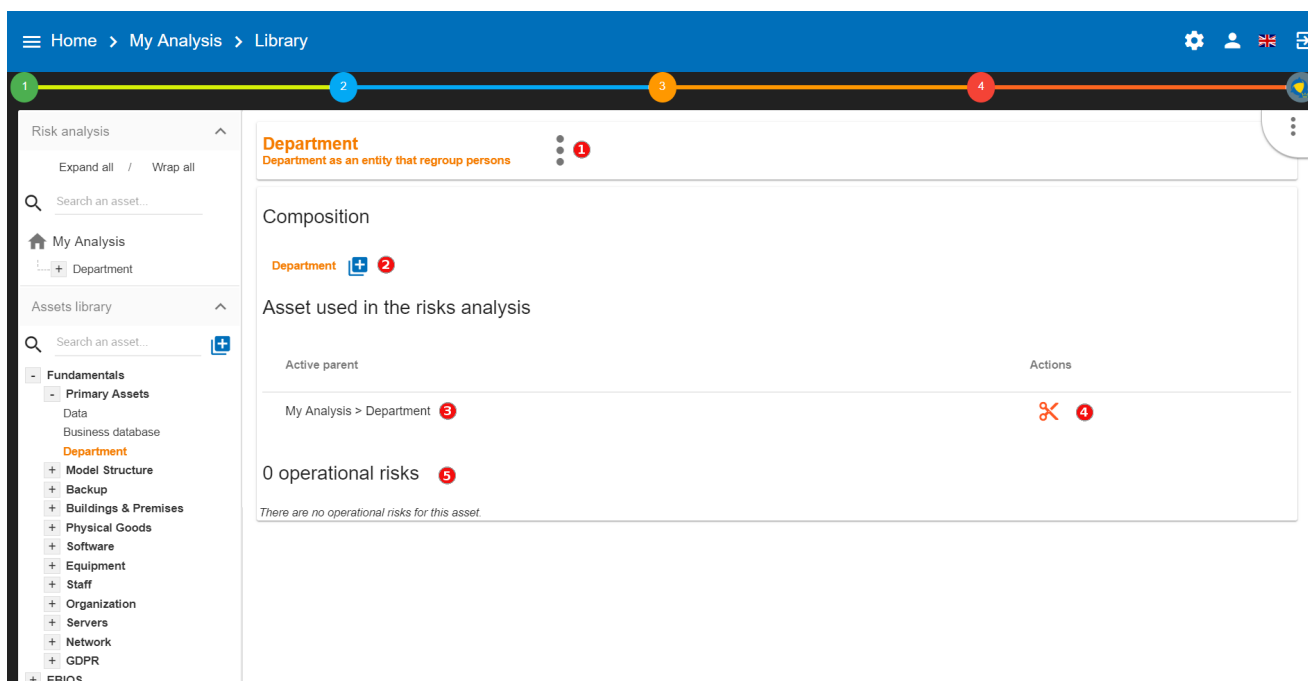
1. Search area in order to quickly find an asset.
2. Button for creating / importing assets (see [Create an Asset](#)).
3. Categories level of the library. There are usually two:
 - a. **Fundamentals**: Contains all default assets offered by CASES.
 - b. **EBIOS**: Contains assets inspired by EBIOS. 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 interface with the 'Building' asset selected. The sidebar on the left contains a tree view of assets, including 'Fundamentals', 'Primary Assets', 'Model Structure', 'Backup', 'Buildings & Premises', 'Company premises', 'Archive room', 'IT room', 'Building', 'Service office', 'Physical Goods', 'Software', 'Equipment', 'Staff', 'Organization', and 'Servers'. The main content area displays the 'Building' asset details, including its composition (Building, Back Office), its use in the risks analysis, and a table of information risks.

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 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.




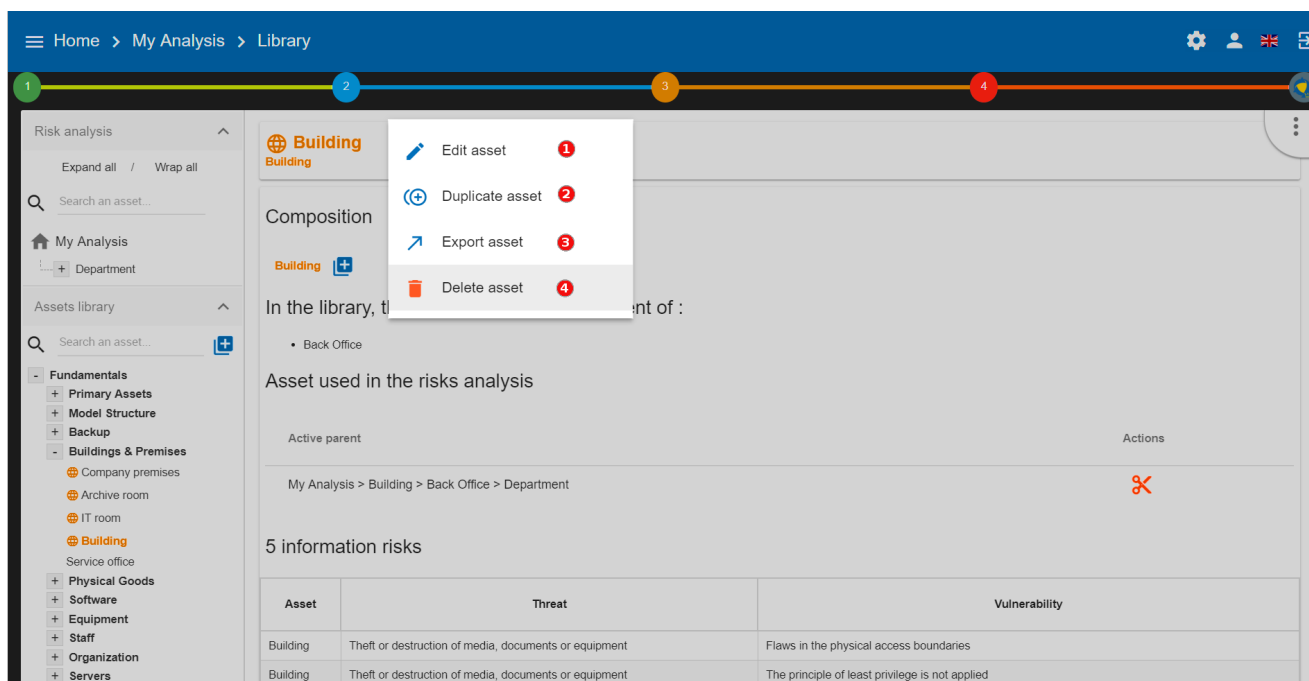
Detach an asset from the analysis will remove all its evaluation.



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.



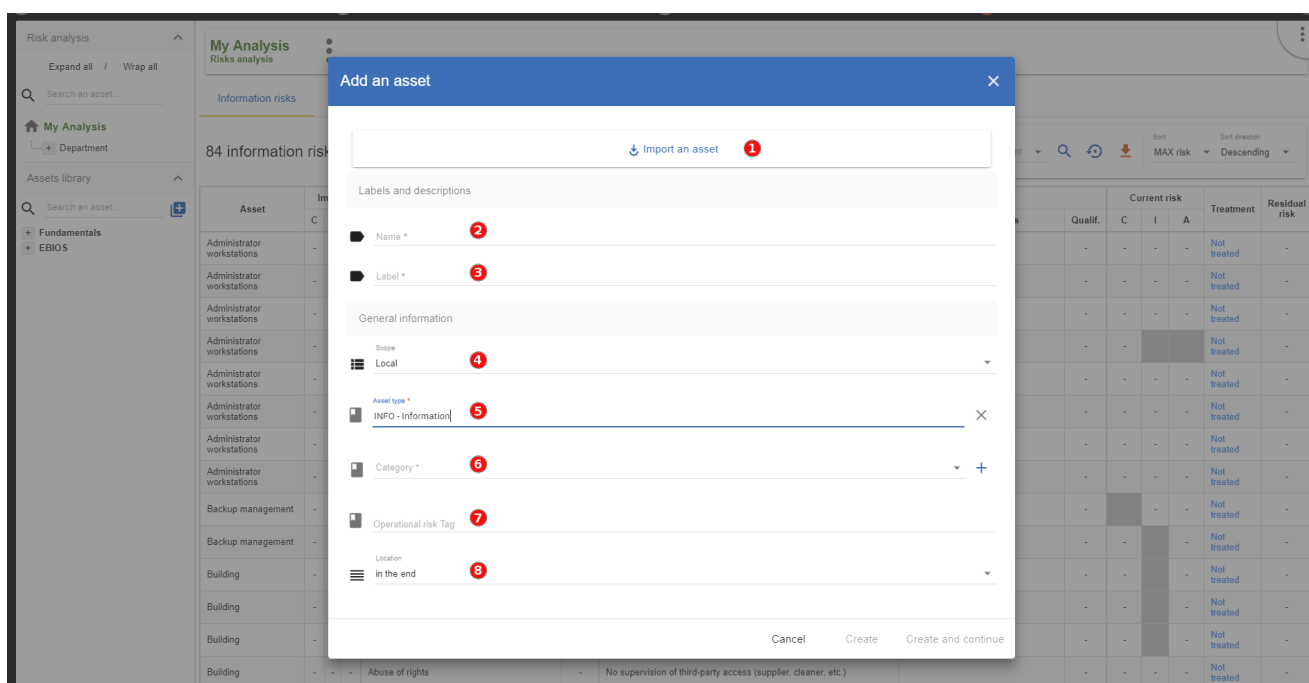
1. Starts the pop-up that allows you to modify most of the parameters of an asset (see [Edit an asset](#)).
2. Create a copy of the asset named **Name (copy #)**, which is then renamed with the **Edit Asset** option.
3. Launches asset export pop-up (see [Exporting an asset](#)).
4. Delete an asset.




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:



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

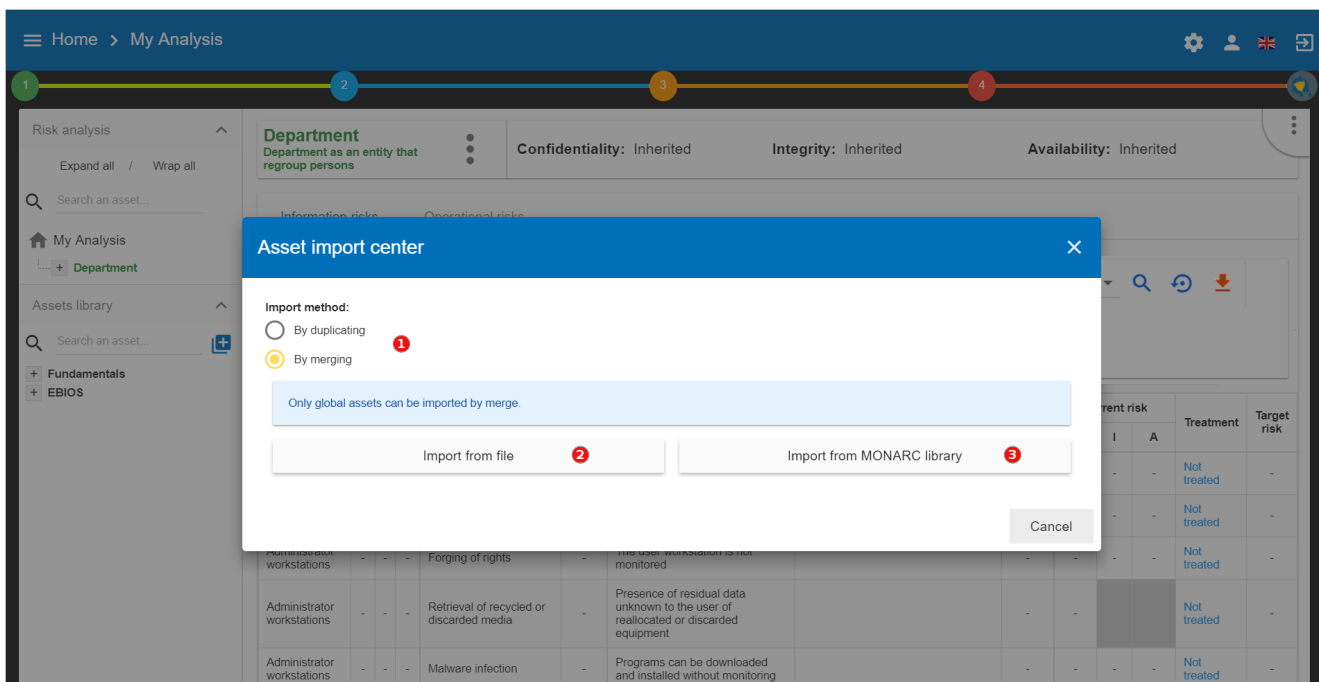
The call is made from the [Context menu of library](#) when an asset is selected in the library.

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](#) 



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.

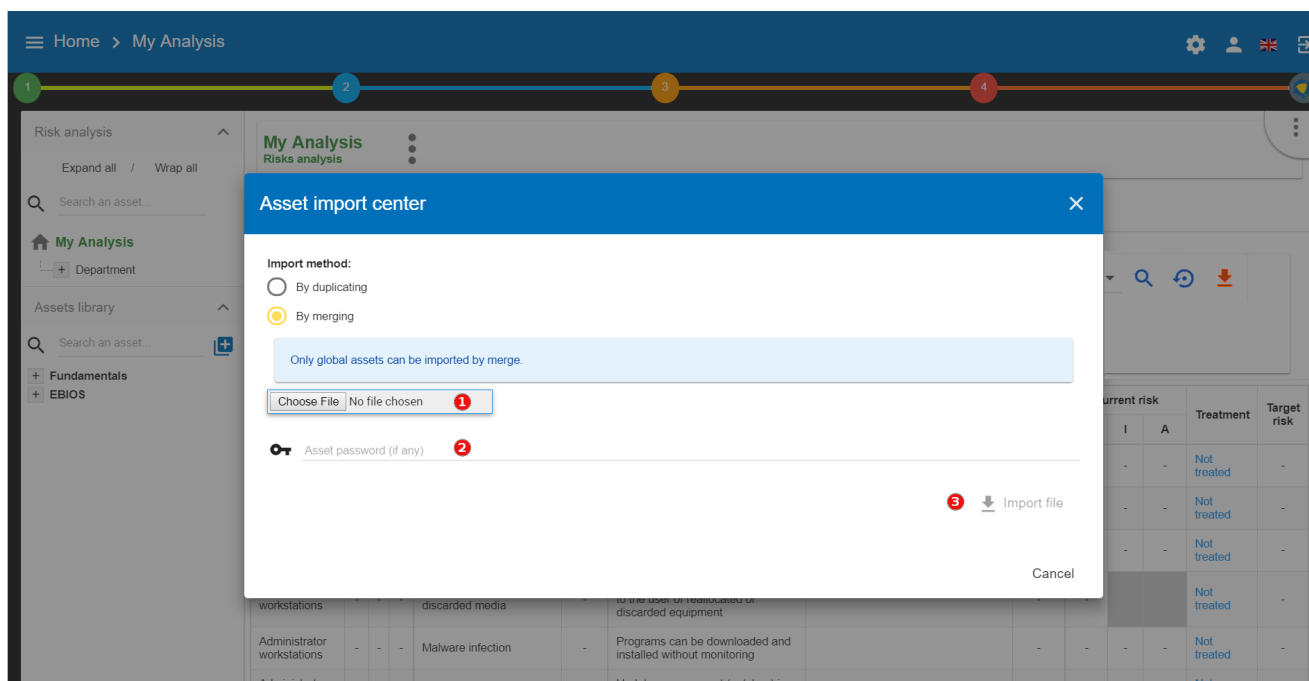
2. **Import from file**: allows to exchange assets from one environment to another (see [Importing an asset from a file](#)).
3. **Import from MONARC library**: This option is not available in the case of a *Stand alone* version of MONARC (see [Import from the MONARC library](#)).



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

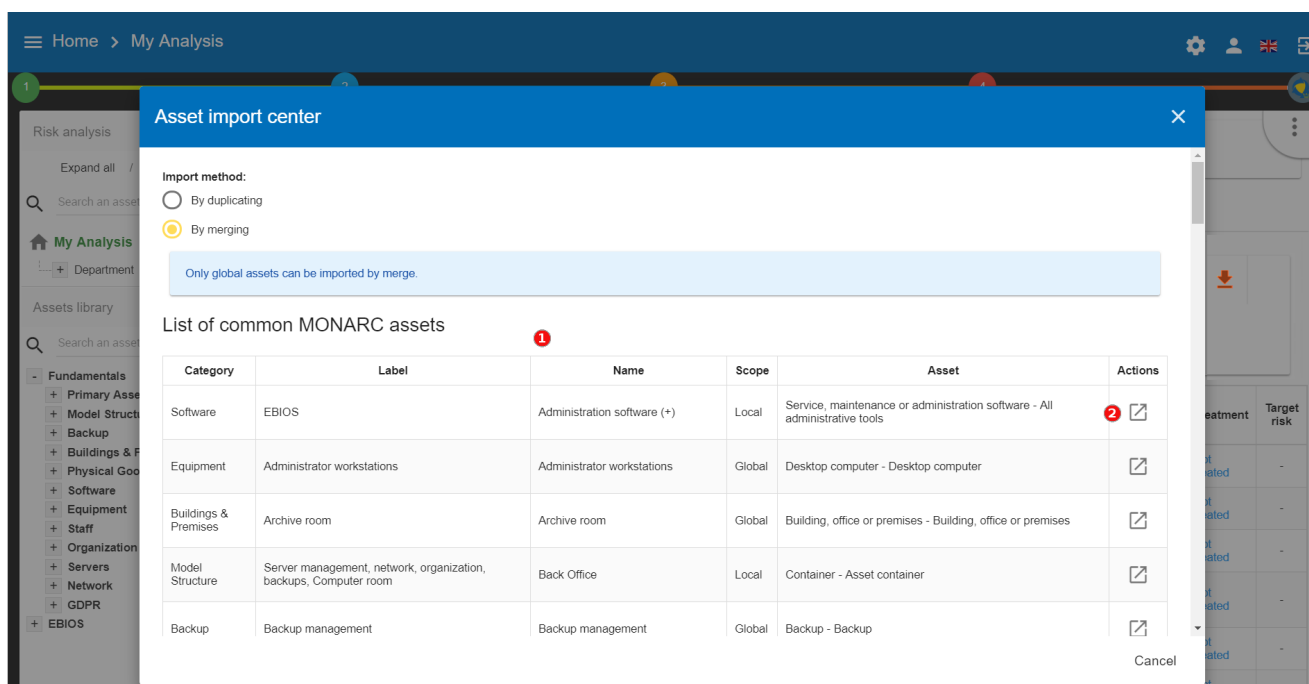
The pop-up appears after clicking on the **Import from file** option in the **Asset Import center**.



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

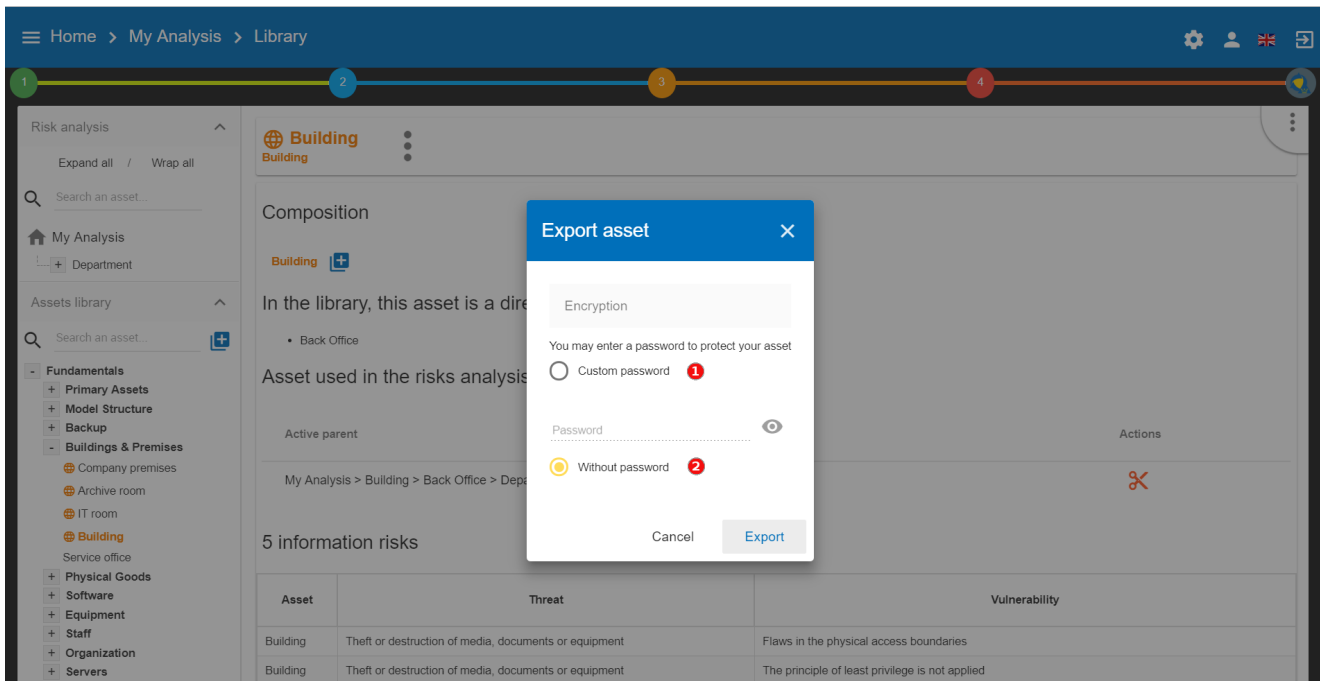
Import from the MONARC library

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



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 the 'Information risks' table displayed. The table has 84 rows of information risks. The columns are: Asset, Impact (C, I, A), Threat (Label, Prob.), Vulnerability (Label, Existing controls, Qualif.), Current risk (C, I, A), Treatment, and Target risk. The table is filtered by 'Risk threshold (on max CIA)' and 'Sort direction' (MAX risk, 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	-	-	-	Malware infection	-	Update management (patches) is		-	-	-	-	Not	-

1. The information risk table based on CIA^[1] criteria.
2. The operational risk table based on ROLFP^[2] (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

The screenshot shows the MONARC interface with the 'My Analysis' page. The sidebar on the left contains a tree view of assets, with 'Department' selected. The main content area has tabs for 'Information risks' and 'Operational risks'. The 'Information risks' tab is active, displaying 84 information risks. The table below shows the details of these risks, including the asset, impact, threat, vulnerability, current risk, treatment, and target risk.

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

2

3

4

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

Type de traitement

Sort

MAX risk

Sort direction

Descending

1 Asset	2 Impact			Threat		Vulnerability			Current risk			Treatment	Residual risk
	C	I	A	Label	3 Prob.	Label	4 Existing controls	5 Qualif.	C	6 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.

The screenshot shows the MONARC Risk Analysis interface. On the left is a sidebar with navigation options: 'Expand all / Wrap all', 'Search an asset...', 'MyPrint EN' (with sub-items: Printing services, Infography Service, GDPR legal obligations), 'Assets library' (with sub-items: Fundamentals, EBIOS), and a search bar. The main content area is titled 'MyPrint EN' and shows 'Information risks' and 'Operational risks' tabs. A 'Back to the list' link is at the top left. The 'Risk sheet' table has columns C, I, and A. Below the table are fields for Threat, Threat probability, Vulnerability, Vulnerability qualification, Existing controls, Recommendations (with a search bar and a plus icon), Kind of treatment (with a dropdown menu), Vulnerability reduction (with a dropdown menu), and Security referentials (with a list of references).

	C	I	A
Current risk	10		40
Residual risk	2		8

Asset: Infography Service > Back office > Backup management

Threat: Theft or destruction of media, documents or equipment

Threat probability: 2 - Unlikely; might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.

Vulnerability: Backup media are not stored in a suitable place

Vulnerability qualification: 5 - Very strong vulnerability: No measures have been implemented. Very low maturity or no maturity at all.

Existing controls: Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.

Recommendations: Search a recommendation

Kind of treatment: 5 Reduction

Vulnerability reduction: 6 1 - Very weak vulnerability: Some efficient measures have been already taken, and their effectiveness is controlled. Very high maturity: Good practices ...

Security referentials: 7 ISO 27002, NIST SP 800-53, 11.2.1 - Equipment siting and protection

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:

Employees
Group of employees

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

6 information risks

Asset	Impact			Threat	Prob.	Vulnerability			Qualif.	Current risk			Treatment	Residual risk
	C	I	A			Label	Existing controls	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 icon , the context menu of asset appears:

Department
Department as an entity that regroup persons

Integrity: 1 Availability: 4

84 information risks

Asset	Impact			Threat	Prob.	Vulnerability			Qualif.	Current risk			Treatment	Residual risk
	C	I	A			Label	Existing controls	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	-	

Context menu options:

- 1 Edit impacts
- 2 Import analysis
- 3 Export analysis
- 4 See asset in the library
- 5 Detach

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.

Edit asset

Consequences Show hidden consequences

	Reputation	Operational	Legal	Financial	Personal	Confidentiality
Confidentiality	2	0	2	Unknown	3	3
Integrity	2	0	1	Unknown	2	2
Availability	2	0	2	Unknown	2	2

Cancel Save

1 Max

3 Strong impact, hardly bearable. Information leaks seriously harm organization

2 Confidential information leaks

1 Bank secrecy

2 Sensitive personal data

3 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 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

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](#).

1

2

3

4

Department

Department as an entity that regroup persons

Confidentiality: 2

Integrity: 2

Availability: 2

Information risks

Operational risks

2 operational risks

Risk threshold (on max NET risk)

Keywords

Kind of treatment

1 Asset	2 Risk description	3 Inherent risk						4 Net risk						5 Existing controls	6 Treatment	7 Residual risk	
		Prob.	Impact					Current risk	Prob.	Impact							Current risk
			R	O	L	F	P			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	2	1	6	Not treated	-
Department	Changes in treatment or further treatment, without prior notification to the data subject	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Not treated	-

+ Create a specific risk

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

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^[3] 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.

1. Back to the list

	Prob.	R	O	L	F	P	MAX risk
Current risk	4	4	4	-	-	-	16
Residual risk	2	1	1	1	1	-	2

2. Current risk

3. Residual risk

4. Risk description

5. Recommendations

6. Kind of treatment

7. Security referentials

Save

1. **Back to the list**: Return to risk table.
2. **Current risk**: Values for risk probability (**Prob.**) and ROLFP^[4] Criteria.
3. **Residual risk**: Values for risk probability and ROLFP^[5] 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
7. Proposals of controls, which come from referentials.



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

The screenshot shows the 'Risk sheet' interface. On the left is a sidebar with 'My Analysis' selected. The main area displays a summary of risks. At the top, there's a 'Back to the list' link. Below it is a table with columns: Prob., R, O, L, F, P, and MAX risk. The table shows 'Current risk' with a value of 6 and 'Residual risk' with a value of 2. 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' (Entry *** > Control all persons in the entrance of the building), and 'Kind of treatment' (Reduction). A 'Save' button is at the bottom right.

	Prob.	R	O	L	F	P	MAX risk
Current risk	2	3	2	2	2	1	6
Residual risk	2	1	1	1	1	0	2

4.4.3. Adding additional risk

When an asset is selected in the analysis:

The screenshot shows the 'Department' asset selected. The main area displays '2 operational risks'. At the top, there are tabs for 'Information risks' and 'Operational risks'. Below the tabs, there's a 'Risk threshold (on max NET risk)' section with a slider and a 'Kind of treatment' dropdown. The table below shows the details of the risks. The first row shows a risk for 'Department' with a 'Current risk' of 12 and a 'Residual risk' of 2. The second row shows a risk for 'Department' with a 'Current risk' of 6 and a 'Residual risk' of 2. A '+ Create a specific risk' button is at the bottom left. The bottom right shows pagination: Page: 1, Rows per page: 20, 1 - 2 of 2.

Asset	Risk description	Inherent risk					Net risk					Existing controls	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	2	1	6	Reduction	2
Department	Changes in treatment or further treatment, without prior notification to the data subject	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Not treated	-

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.

[1] CIA, Confidentiality, Integrity and Availability.

[2] rolfp, Reputation, Operational, Legal, Financial and Personal

[3] rolfp

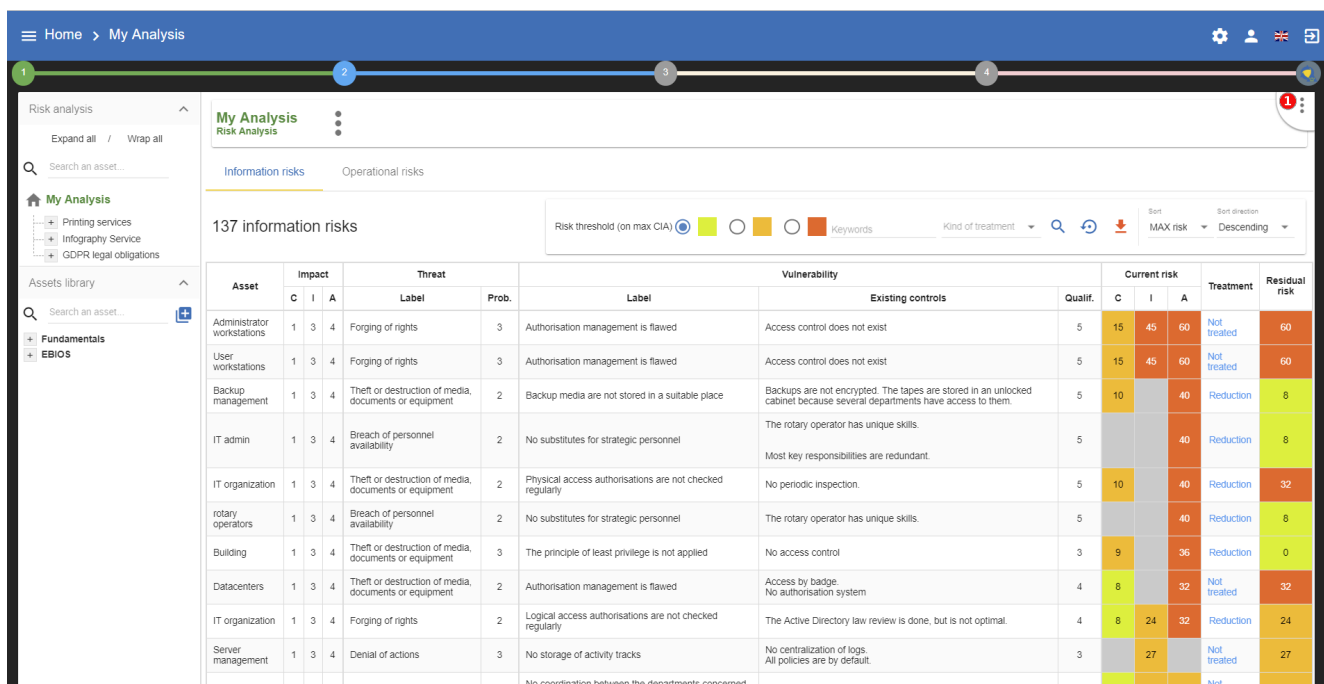
[4] rolfp

[5] rolfp

Chapter 5. Evaluation Scales

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

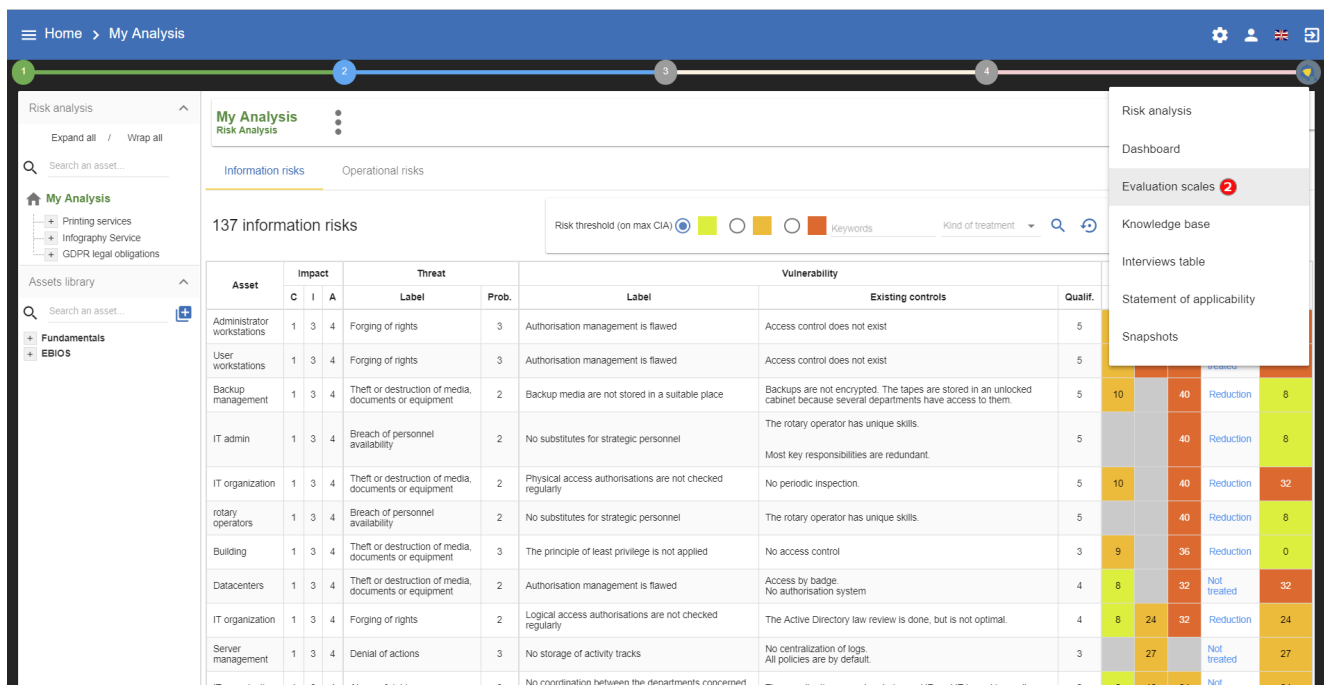
1. Calling the right contextual menu



The screenshot shows the 'My Analysis' page with the 'Information risks' section active. The table displays 137 information risks. The table structure is as follows:

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Label	Existing controls		C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.		5	10		40	Reduction	8
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.		5			40	Reduction	8
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.		5	10		40	Reduction	32
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.		5			40	Reduction	8
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control		3	9		36	Reduction	0
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system		4	8		32	Not treated	32
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.		4	8	24	32	Reduction	24
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.		3		27		Not treated	27
IT organization	1	3	4	Denial of rights	3	No coordination between the departments concerned	The coordination procedure between HQ and IT is working well		2	6	18	24	Not	24

2. Calling the Management view of Evaluation scales



The screenshot shows the 'My Analysis' page with the 'Information risks' section active. A dropdown menu is open, showing the 'Evaluation scales' option highlighted with a red circle '2'. The table structure is the same as in the previous screenshot.

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

Home > My Analysis > Evaluation scales

Impacts scale: [0 - 4]

Show hidden impacts

	Confidentiality	Integrity	Availability	Reputation	Operational	Personal	New column name
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. Examples: - 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.	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. Examples: - 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 easy to rectify without any 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 not reached.	Temporary degradation of the company or staff reputation. Occasional media critics	Isolated incidents with a manageable impact on customers.	Significant 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.	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:	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.	Significant 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 brings 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: - 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 maximums time periods consider as unbearable.	Death of someone. Definitive degradation of the company or staff reputation. International media coverage.	Complete stop of all services	Significative 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 2

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

8

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

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 2

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

8

27

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

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

4 0 4 8 12 16 20 24 32 36 40 48 60 64 80

R = I x (T x V)

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

Acceptance thresholds of operational risks

3

0 1 2 3 4

0 0 0 0 0 0

1 0 1 2 3 4

2 0 1 2 3 4

R = I x P

R: Risk, I: Impact, P: 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 - 6]

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

8

1

27

TxV

00000000000000

00123456891012151620

0000000000000000

00123456891012151620

002468101216182024303240

0036912151824273036454860

00481216202432364048606480

R = I x (T x V)

2

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

Acceptance thresholds of operational risks

3

3

8

Probability

000000

001234

00000000

001234

002468

0036912

00481216

R = I x P

4

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**

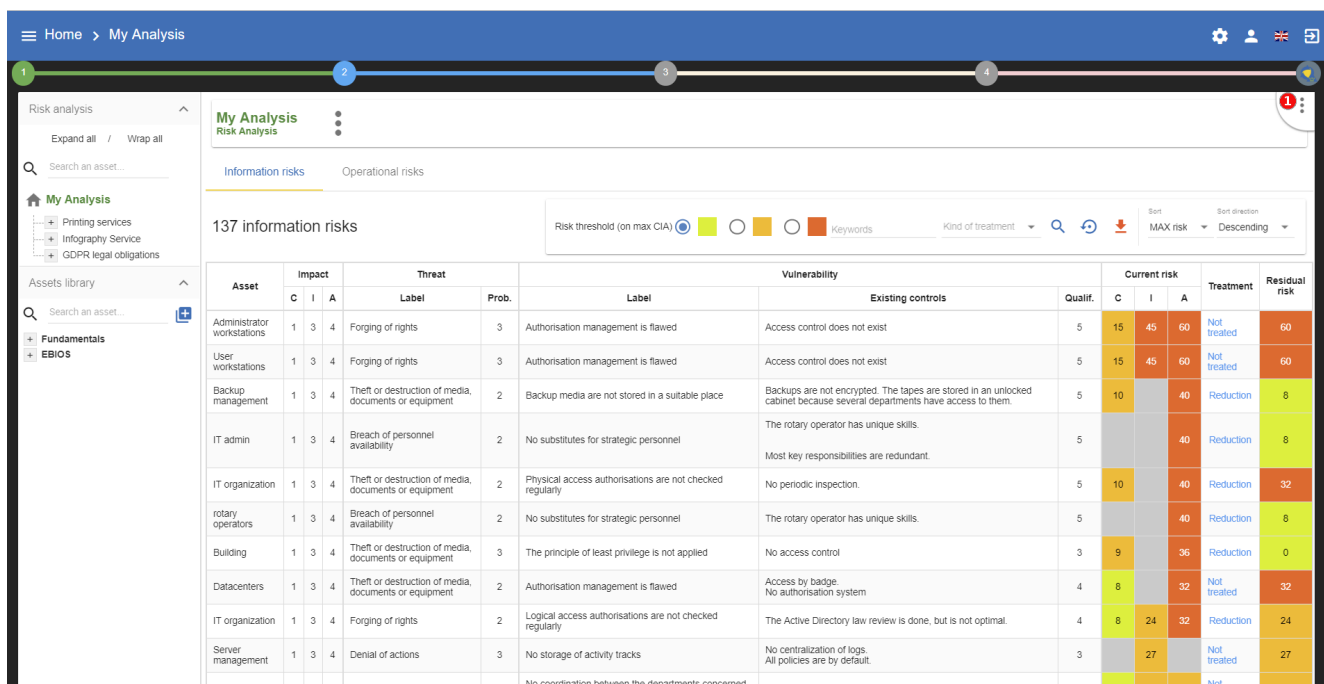
CASES Luxembourg

Page 36 / 61

Chapter 6. Management of Knowledge Base

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





1. Calling the right contextual menu



My Analysis Risk Analysis

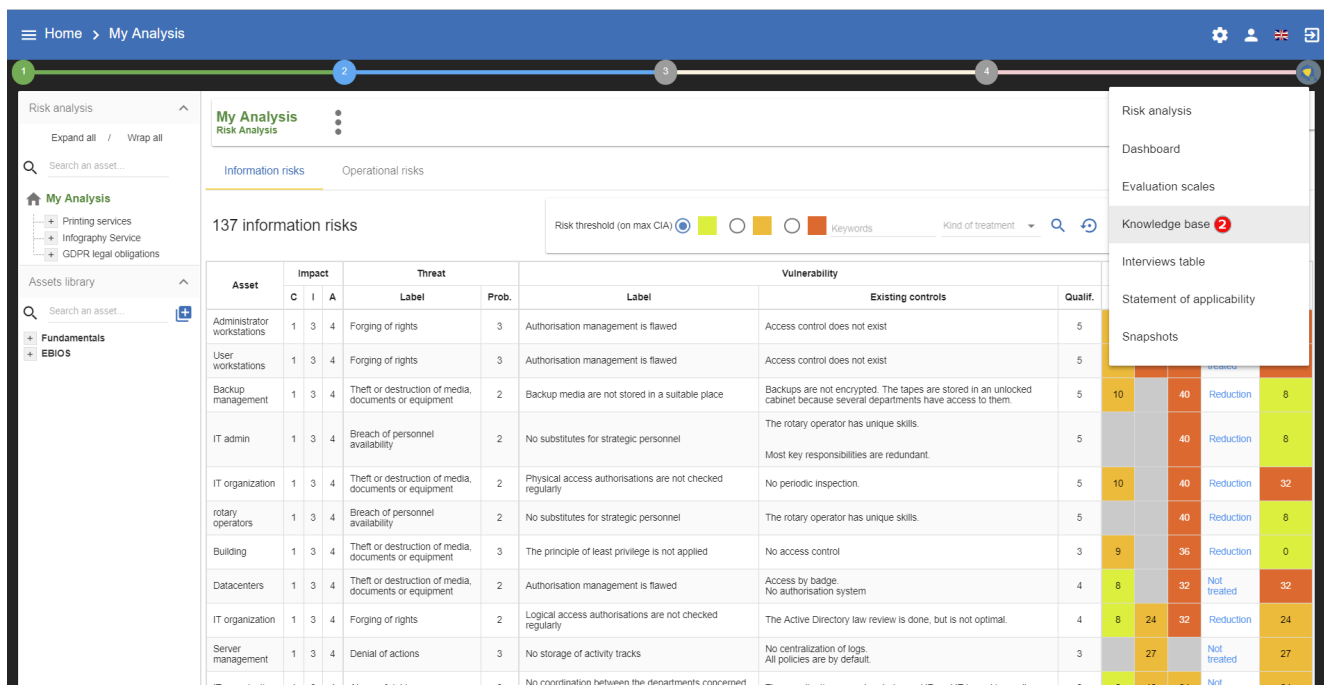
Information risks Operational risks

137 information risks

Risk threshold (on max CIA)  Keywords Kind of treatment   Sort MAX risk  Sort direction Descending

Asset	Impact			Threat	Prob.	Label	Vulnerability	Existing controls	Qualif.	Current risk			Treatment	Residual risk
	C	I	A							C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist	5	15	45	60	Not treated	60	
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist	5	15	45	60	Not treated	60	
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.	5	10	40	40	Reduction	8	
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.	5		40	40	Reduction	8	
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.	5	10	40	40	Reduction	32	
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.	5		40	40	Reduction	8	
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control	3	9	36	36	Reduction	0	
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system	4	8	32	32	Not treated	32	
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.	4	8	24	32	Reduction	24	
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.	3		27	27	Not treated	27	
IT organization	1	3	4	Denial of rights	3	No coordination between the departments concerned	The coordination procedure between HQ and IT is working well	2	6	18	24	Not	24	





2. Calling the Management view of Knowledge base



My Analysis Risk Analysis

Information risks Operational risks

137 information risks

Risk threshold (on max CIA)  Keywords Kind of treatment   Sort MAX risk  Sort direction Descending

Knowledge base

- Risk analysis
- Dashboard
- Evaluation scales
- Knowledge base**
- Interviews table
- Statement of applicability
- Snapshots

All parameters are managed with the same view:

Home > My Analysis > Knowledge base

Asset types 1 Threats Vulnerabilities 27002 controls Information risks Tags Operational risks

Asset types 2 Search 3 Show active only

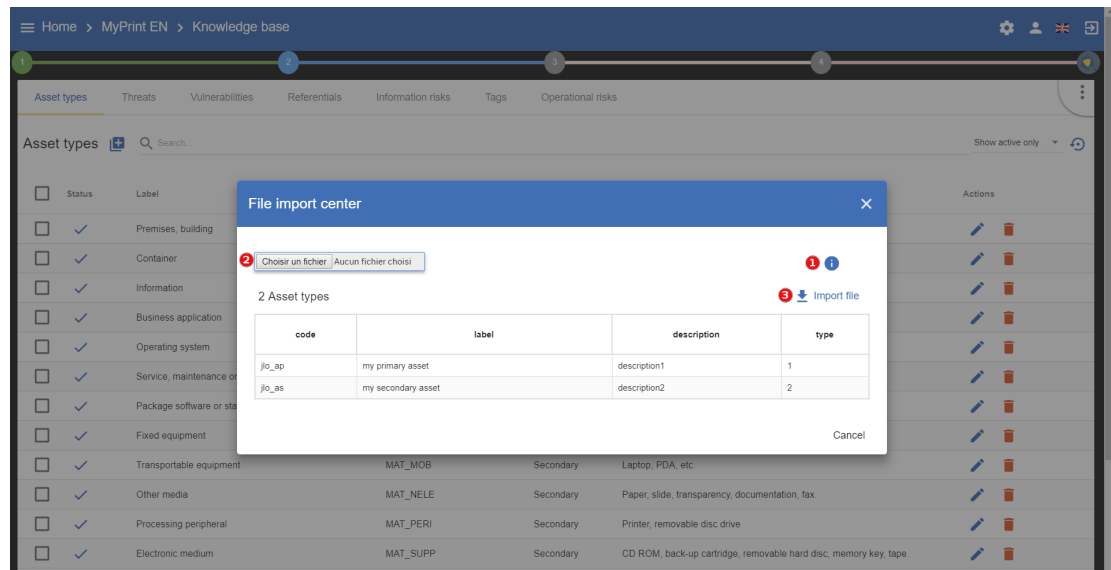
4	Status	Label	Code	Type	Description	5
<input type="checkbox"/>	✓	Company directory	SYS_ANU	Secondary	Company directory	
<input type="checkbox"/>	✓	Business application	LOG_APP	Secondary	Custom business application or standard	
<input type="checkbox"/>	✓	Other media	MAT_NELE	Secondary	Paper, slide, transparency, 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.

When adding an item, all the tabs (except information risks) have the possibility to add items from external files (click at the top of the pop-up on Import from files).



1. Display all the information needed to create the right file.
2. Upload the file.
3. Import it.

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 using 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 themes 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. Referentials

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

The screenshot shows the MONARC Knowledge base interface. The top navigation bar includes tabs for Asset types, Threats, Vulnerabilities, Referentials, Information risks, Tags, and Operational risks. The main content area displays a list of controls under the heading 'Controls'. The controls are listed in a table with columns for Code, Label, Category, and Actions. The controls are numbered 1 through 12, corresponding to the numbered callouts in the text below.

Code	Label	Category	Actions
5.1.1	Policies for information security	Information security policies	[Edit] [Delete]
5.1.2	Review of the policies for information security	Information security policies	[Edit] [Delete]
6.1.1	Information security roles and responsibilities	Organization of information security	[Edit] [Delete]
6.1.2	Segregation of duties	Organization of information security	[Edit] [Delete]
6.1.3	Contact with authorities	Organization of information security	[Edit] [Delete]
6.1.4	Contact with special interest groups	Organization of information security	[Edit] [Delete]
6.1.5	Information Security in Project Management	Organization of information security	[Edit] [Delete]
6.2.1	Mobile device policy	Organization of information security	[Edit] [Delete]
6.2.2	Teleworking	Organization of information security	[Edit] [Delete]
7.1.1	Screening	Human resource security	[Edit] [Delete]
7.1.2	Terms and conditions of employment	Human resource security	[Edit] [Delete]

1. This area is dedicated to manage the selection of referential. In the right, there are the standard buttons to edit, add and delete a referential.
2. This new icon appears when you have two referential, it allows you to add, import or export matching between the selected referential and the others.
3. This area is dedicated so manage security controls of the selected referential.

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 security measures from the referentials tabs. Only supporting assets are available for a Threat / Vulnerability association.

1. It is possible to switch between referential to see its linked controls of the risks show below.
2. This new icon appears when you have two referential, it allows you to automatically linked controls of a referential to risks. It uses the matching defined in the step before.

1. The first referential is the one which you want to link to the risks.
2. The second is the source you want to use (it has taken risks linked to its controls).

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. It is possible to link security controls as for the risks of the information.

6.8. Recommendations Sets

It is the repository that is used by default to manage the recommendations.

The screenshot displays the 'Recommendations Sets' interface in the MONARC application. The top navigation bar includes tabs for 'Asset types', 'Threats', 'Vulnerabilities', 'Referentials', 'Information risks', 'Tags', 'Operational risks', and 'Recommendations Sets'. The 'Recommendations Sets' tab is selected, showing a list of recommendations. The list has columns for 'Status', 'Code', 'Description', 'Importance', and 'Actions'. A search bar and a 'Show active only' filter are located at the top right of the list. The list contains 15 recommendations, each with a status icon (checkmark or cross), a code (e.g., Rec 1, Rec 10, Rec 11), a description, an importance level (indicated by red dots), and action icons (edit and delete).

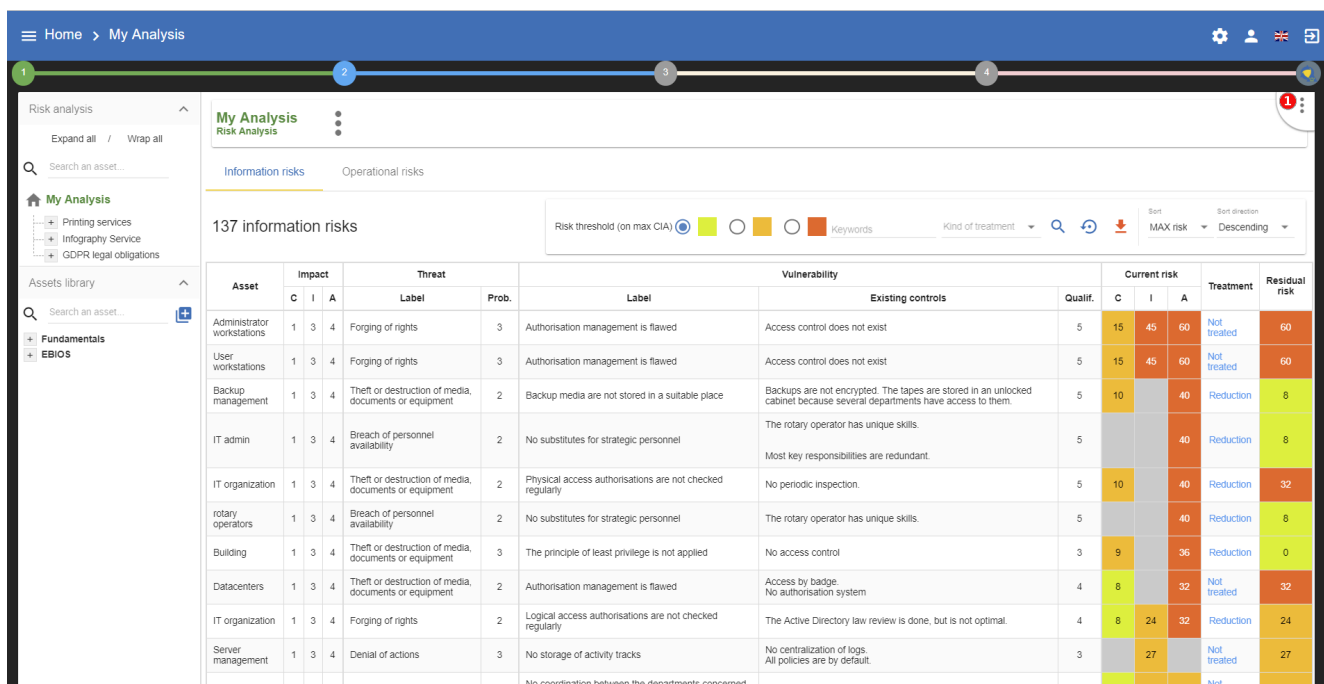
Status	Code	Description	Importance	Actions
✓	Rec 1	Define the rules for using and leaving the equipment, for all staff.	•	[Edit] [Delete]
✓	Rec 10	Implement rigorous access control including the need to know	•••	[Edit] [Delete]
✓	Rec 11	Implement a centralized authentication system for workstations	••	[Edit] [Delete]
✓	Rec 12	Designate a DPO compliant with the GDPR	••	[Edit] [Delete]
✓	Rec 13	Establish a procedure to keep applicants informed of the consideration of their request and the processing	••	[Edit] [Delete]
✓	Rec 14	Identify the personal data necessary for the purpose of the processing and justify why each category of personal data is essential	••	[Edit] [Delete]
✓	Rec 15	List in a register the processing of personal data and keep it up to date	••	[Edit] [Delete]
✓	Rec 2	Accompany external people for any intervention in the Datacenter.	••	[Edit] [Delete]
✓	Rec 3	Provide access by badge and write a note prohibiting the door from being blocked.	•••	[Edit] [Delete]
✓	Rec 4	Define a maintenance procedure that prevents aging of the equipment.	•••	[Edit] [Delete]
✓	Rec 5	Train at least one additional person in the use of the machines.	•••	[Edit] [Delete]
✓	Rec 6	Periodically review access authorizations.	••	[Edit] [Delete]
✓	Rec 7	Periodically test the restoration procedure using a representative sample of data.	•••	[Edit] [Delete]

1. This area is dedicated to manage the selection of sets of recommendations. In the right, there are the standard buttons to edit, add and delete a referential.
2. This area is dedicated so manage recommendations of the selected set.

Chapter 7. Statement of applicability

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

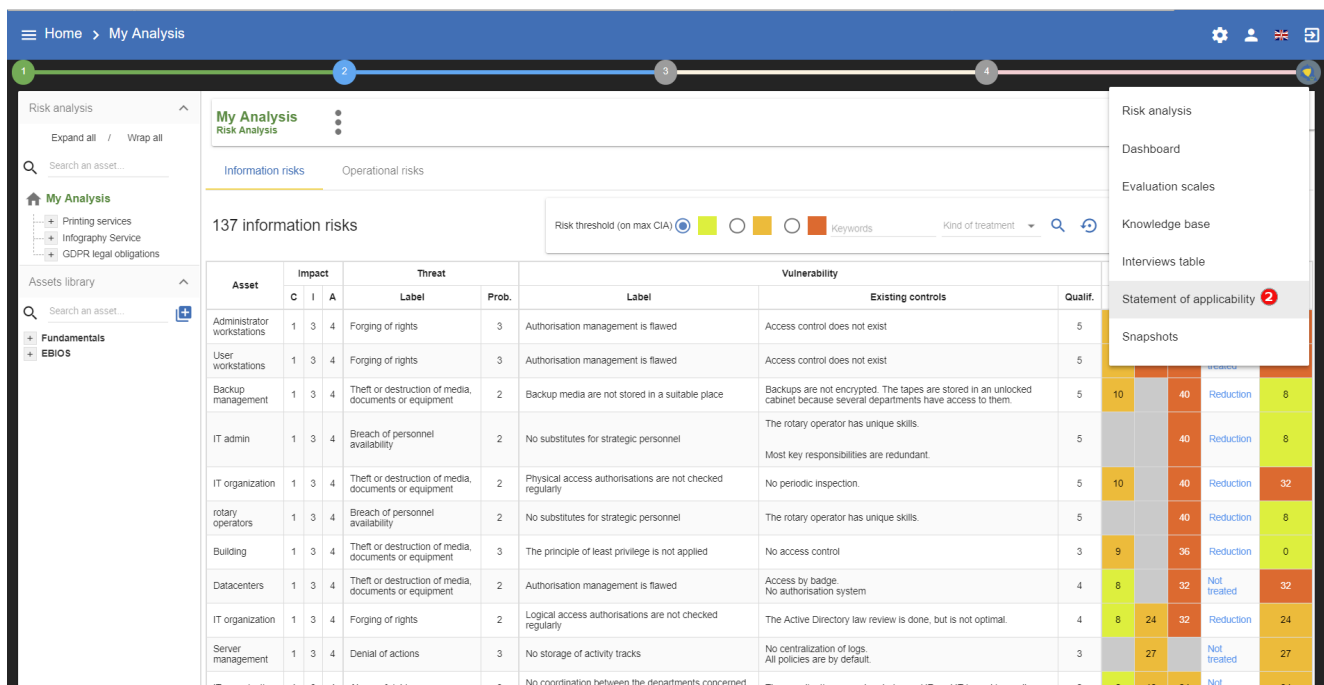
1. Calling the right contextual menu



The screenshot shows the 'My Analysis' page with the 'Information risks' tab selected. The table displays 137 information risks. A red circle '1' is placed over the three-dot menu icon in the top right corner of the 'My Analysis' header.

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Label	Existing controls		C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.		5	10		40	Reduction	8
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.		5			40	Reduction	8
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.		5	10		40	Reduction	32
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.		5			40	Reduction	8
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control		3	9		36	Reduction	0
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system		4	8		32	Not treated	32
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.		4	8	24	32	Reduction	24
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.		3		27		Not treated	27
IT organization	1	3	4	Denial of rights	3	No coordination between the departments concerned	The coordination procedure between HQ and IT is working well		2	6	18	24	Not	24

2. Calling the Management view of Statement of applicability



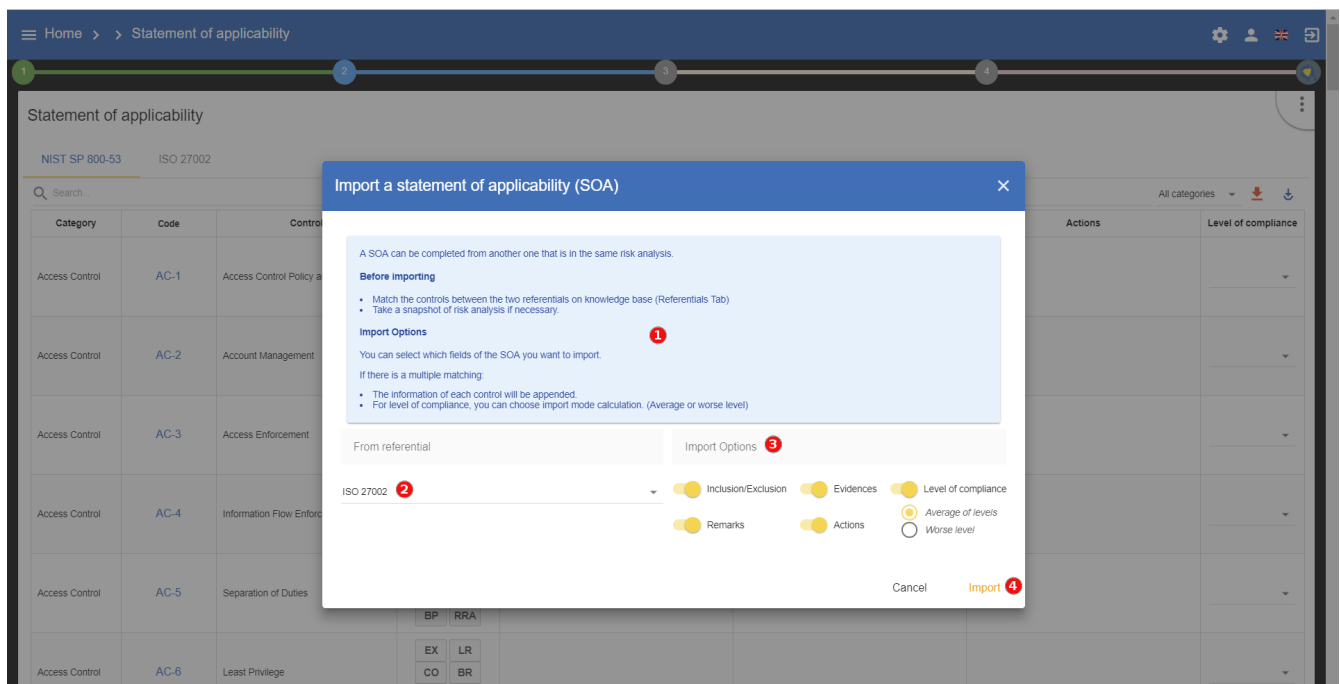
The screenshot shows the 'My Analysis' page with the 'Information risks' tab selected. A dropdown menu is open, showing various options. A red circle '2' is placed over the 'Statement of applicability' option.

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Label	Existing controls		C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.		5	10		40	Reduction	8
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.		5			40	Reduction	8
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.		5	10		40	Reduction	32
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.		5			40	Reduction	8
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control		3	9		36	Reduction	0
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system		4	8		32	Not treated	32
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.		4	8	24	32	Reduction	24
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.		3		27		Not treated	27
IT organization	1	3	4	Denial of rights	3	No coordination between the departments concerned	The coordination procedure between HQ and IT is working well		2	6	18	24	Not	24

The view **Statement of applicability** above:

1. Choose the **referential** on which one you want to work.
2. The **code** is a clickable field, click on it and see all the risks attached to the security control selected.

3. Choose if the security control is **included or excluded**, just click on the acronym, the description of it appears if the cursor is on it.
4. The field **remarks/justification**, **Evidences**, **Actions** are text field, just click on it and fill.
5. The **Level of compliance** is a drop-down list.
6. **Export** the selected view in CSV.
7. **Import** information for the selected referential from another.

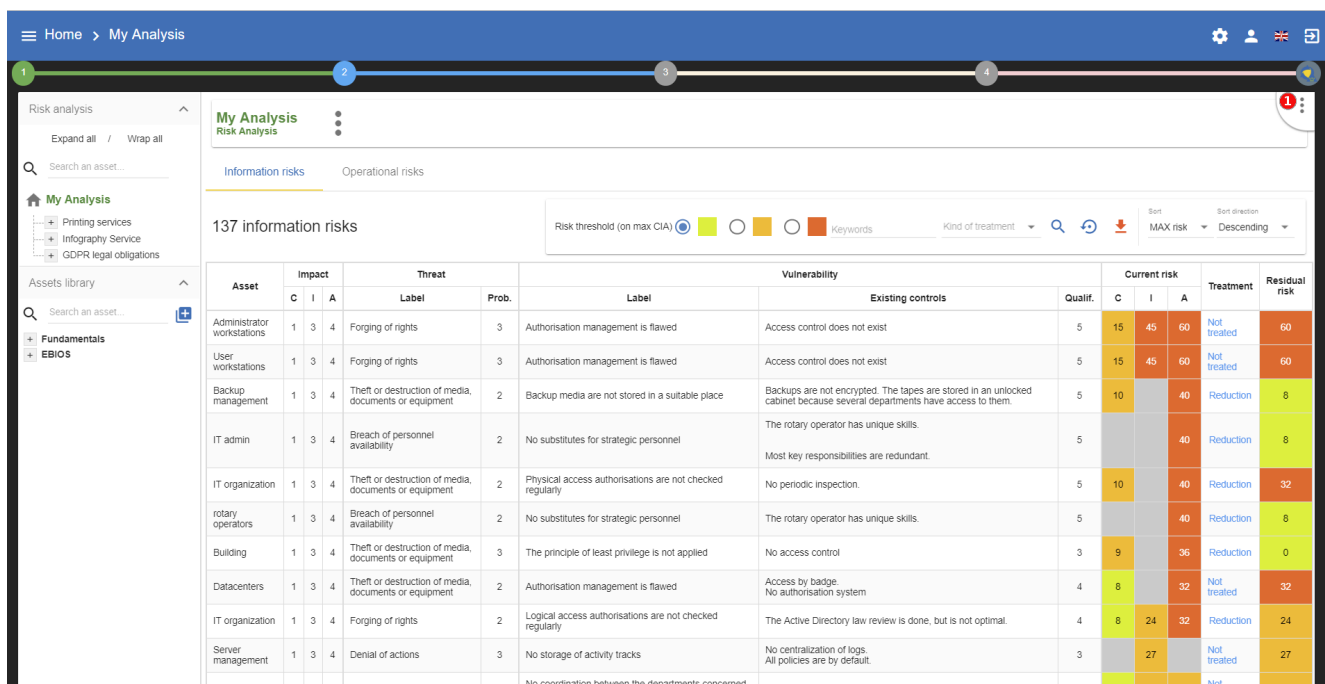


1. **Read** what you are willing to do.
2. Choose the **referential** which contains information that you want to convert into the selected one.
3. Choose **information** you want to import.
4. **Import** the information of the referential.

Chapter 8. Dashboard

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




1. Calling the right contextual menu



My Analysis Risk Analysis

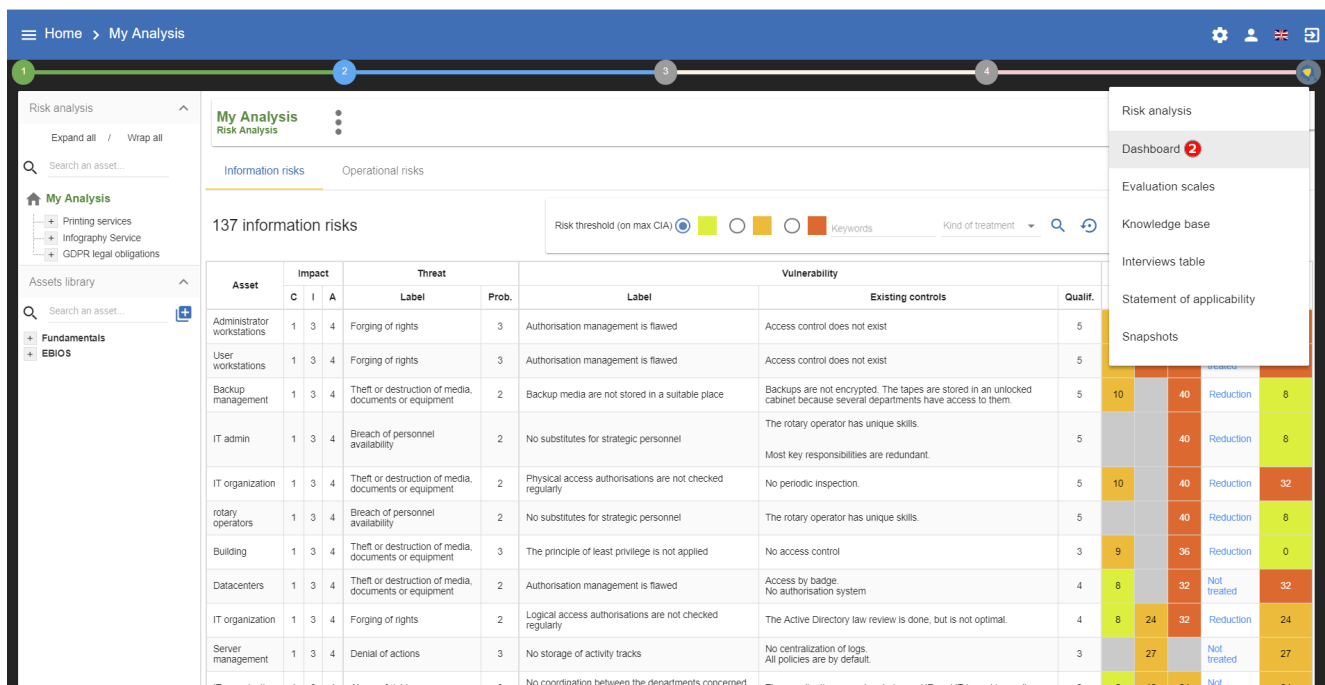
Information risks Operational risks

137 information risks

Risk threshold (on max CIA)  Keywords Kind of treatment   Sort MAX risk Sort direction Descending

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Label	Existing controls		C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.		5	10		40	Reduction	8
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.		5			40	Reduction	8
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.		5	10		40	Reduction	32
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.		5			40	Reduction	8
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control		3	9		36	Reduction	0
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system		4	8		32	Not treated	32
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.		4	8	24	32	Reduction	24
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.		3		27		Not treated	27
IT organization	1	3	4	Denial of rights	3	No coordination between the departments concerned	The coordination procedure between HQ and IT is working well		2	6	18	24	Not	24




2. Calling the Management view of Dashboard



My Analysis Risk Analysis

Information risks Operational risks

137 information risks

Risk threshold (on max CIA)  Keywords Kind of treatment   Sort MAX risk Sort direction Descending

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Label	Existing controls		C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.		5	10		40	Reduction	8
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.		5			40	Reduction	8
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.		5	10		40	Reduction	32
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.		5			40	Reduction	8
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control		3	9		36	Reduction	0
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system		4	8		32	Not treated	32
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.		4	8	24	32	Reduction	24
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.		3		27		Not treated	27
IT organization	1	3	4	Denial of rights	3	No coordination between the departments concerned	The coordination procedure between HQ and IT is working well		2	6	18	24	Not	24

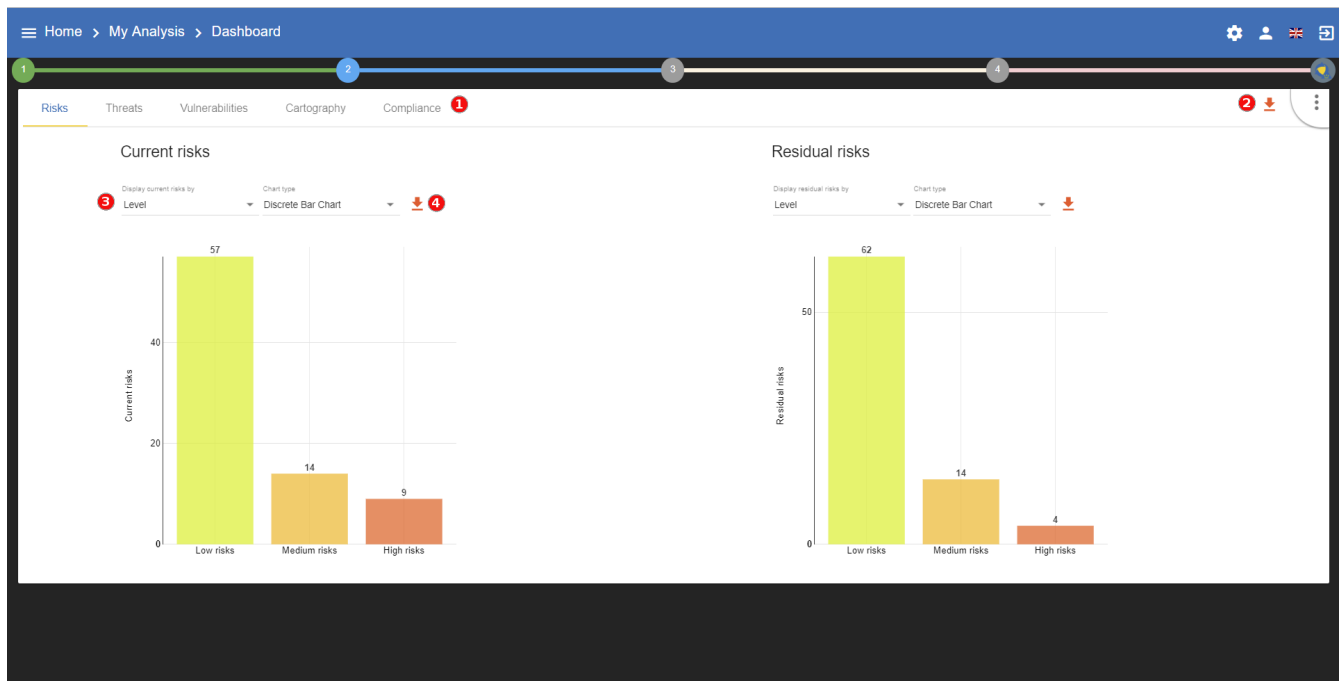
The view **Dashboard** shows informations about the following topics:

- Risks
- Threats
- Vulnerabilities

- Cartography
- Compliance



Most of the charts have parameters and are exportable.



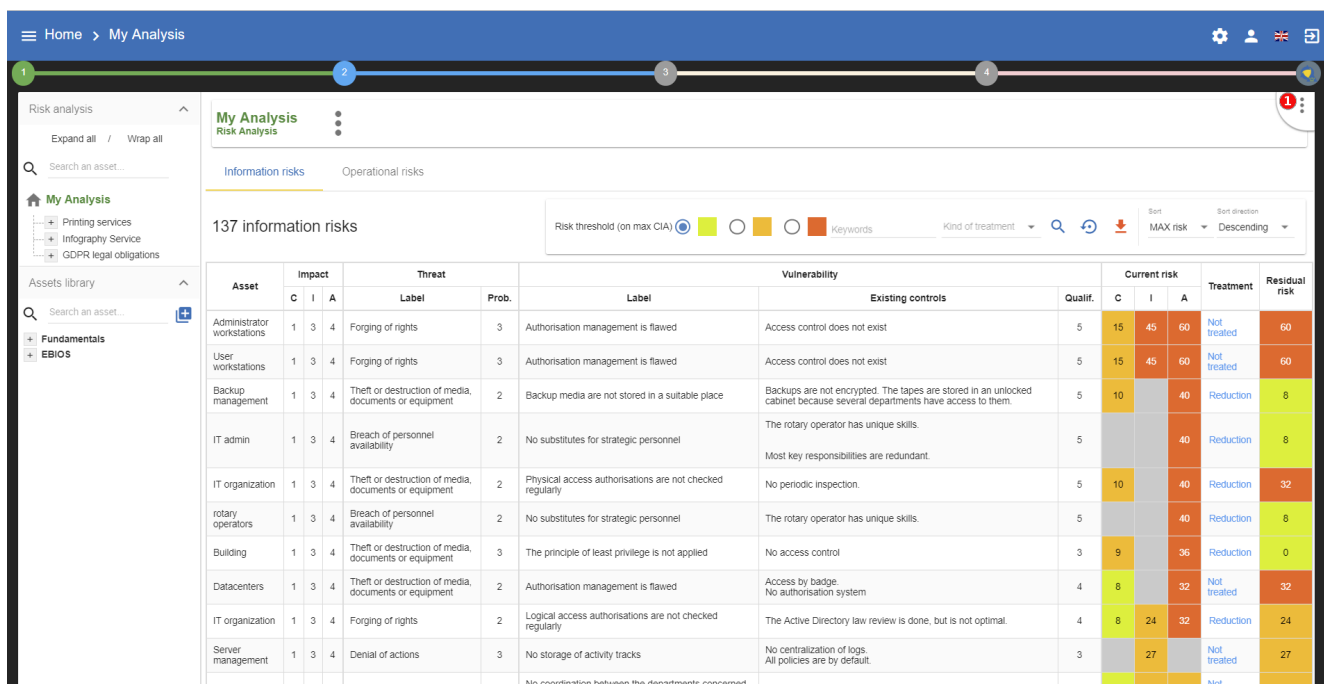
All the part of the dashboard have the same functionalities.

1. **Choose** the part on which dashboard is required.
2. **Export** all the data in a XLSX document to make your own graph.
3. **Change** the paramaters of the selected chart.
4. **Export** the chart as PNG

Chapter 9. Record of processing activities

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

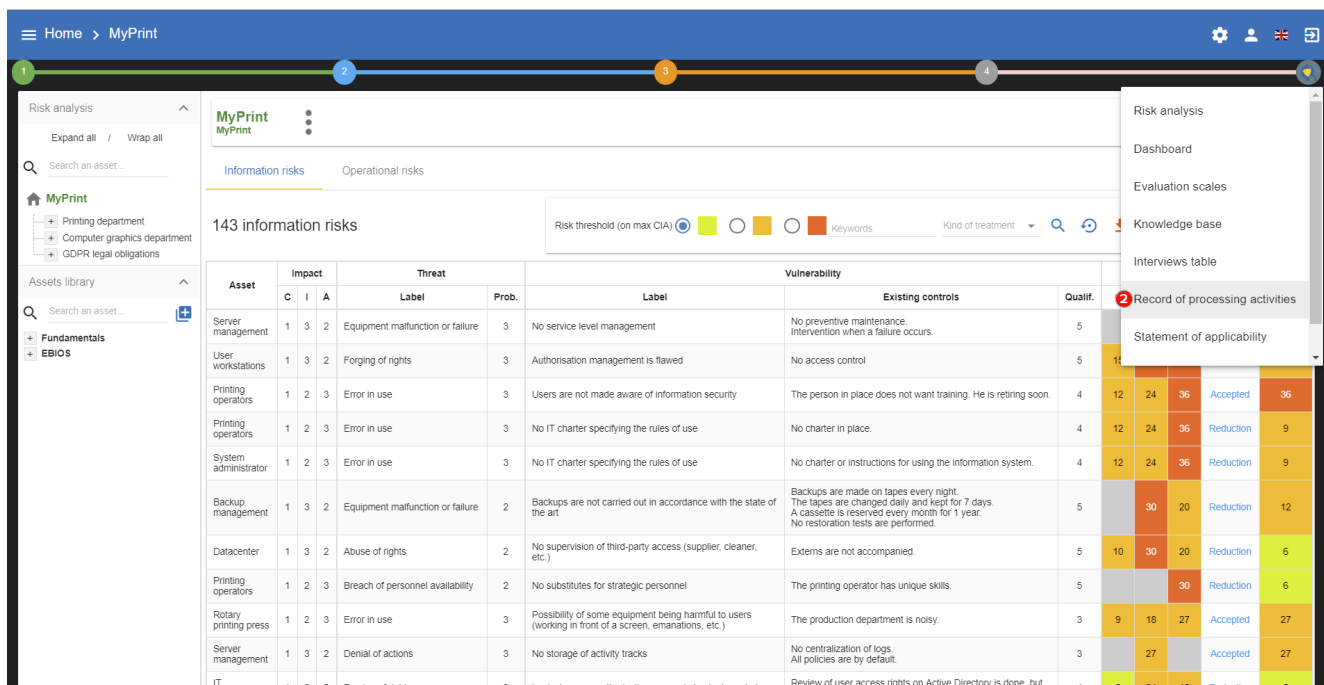
1. Calling the right contextual menu



The screenshot shows the 'My Analysis' interface. On the left, there's a sidebar with 'Risk analysis' and 'Assets library'. The main area displays '137 information risks'. A table lists various assets and their associated risks. A contextual menu is open on the right, with 'Record of processing activities' highlighted by a red circle and a red arrow.

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Existing controls	C		I	A			
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist	5	15	45	60	Not treated	60	
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist	5	15	45	60	Not treated	60	
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.	5	10	40	40	Reduction	8	
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.	5		40	40	Reduction	8	
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.	5	10	40	40	Reduction	32	
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.	5		40	40	Reduction	8	
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control	3	9	36	36	Reduction	0	
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system	4	8	32	32	Not treated	32	
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.	4	8	24	32	Reduction	24	
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.	3		27	27	Not treated	27	
IT organization	1	3	4	Abuse of rights	2	No coordination between the departments concerned	The coordination procedure between IAD and IT is working well	2	6	18	24	Not	24	

2. Calling the Management view of Record of processing activities



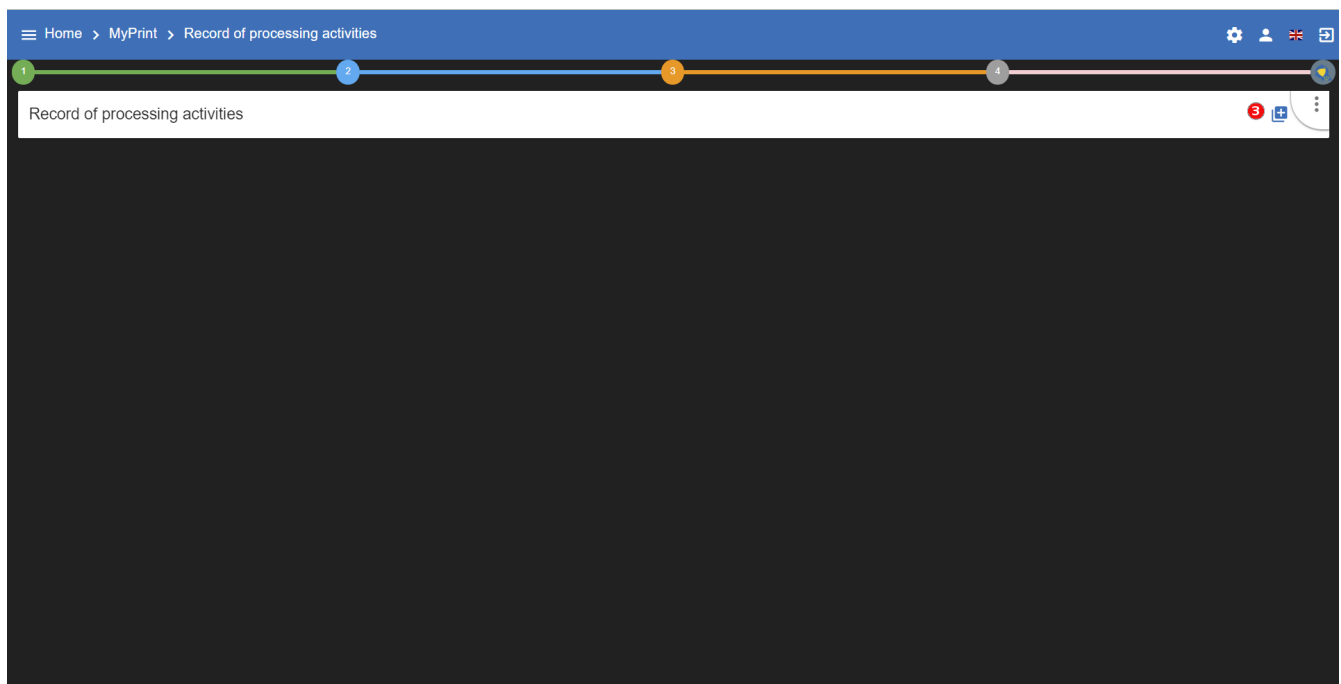
The screenshot shows the 'MyPrint' interface. On the left, there's a sidebar with 'Risk analysis' and 'Assets library'. The main area displays '143 information risks'. A table lists various assets and their associated risks. A contextual menu is open on the right, with 'Record of processing activities' highlighted by a red circle and a red arrow.

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Existing controls	C		I	A			
Server management	1	3	2	Equipment malfunction or failure	3	No service level management	No preventive maintenance. Intervention when a failure occurs.	5						
User workstations	1	3	2	Forging of rights	3	Authorisation management is flawed	No access control	5	15	45	60	Not treated	60	
Printing operators	1	2	3	Error in use	3	Users are not made aware of information security	The person in place does not want training. He is retiring soon.	4	12	24	36	Accepted	36	
Printing operators	1	2	3	Error in use	3	No IT charter specifying the rules of use	No charter in place.	4	12	24	36	Reduction	9	
System administrator	1	2	3	Error in use	3	No IT charter specifying the rules of use	No charter or instructions for using the information system.	4	12	24	36	Reduction	9	
Backup management	1	3	2	Equipment malfunction or failure	2	Backups are not carried out in accordance with the state of the art	Backups are made on tapes every night. The tapes are changed daily and kept for 7 days. A cassette is reserved every month for 1 year. No restoration tests are performed.	5		30	20	Reduction	12	
Datacenter	1	3	2	Abuse of rights	2	No supervision of third-party access (supplier, cleaner, etc.)	Externs are not accompanied.	5	10	30	20	Reduction	6	
Printing operators	1	2	3	Breach of personnel availability	2	No substitutes for strategic personnel	The printing operator has unique skills.	5		30	30	Reduction	6	
Rotary printing press	1	2	3	Error in use	3	Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	The production department is noisy.	3	9	18	27	Accepted	27	
Server management	1	3	2	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.	3		27	27	Accepted	27	
IT	1	3	2	Forging of rights	2	Logical access authorisations are not checked regularly	Review of user access rights on Active Directory is done, but	4	8	24	36	Reduction	6	



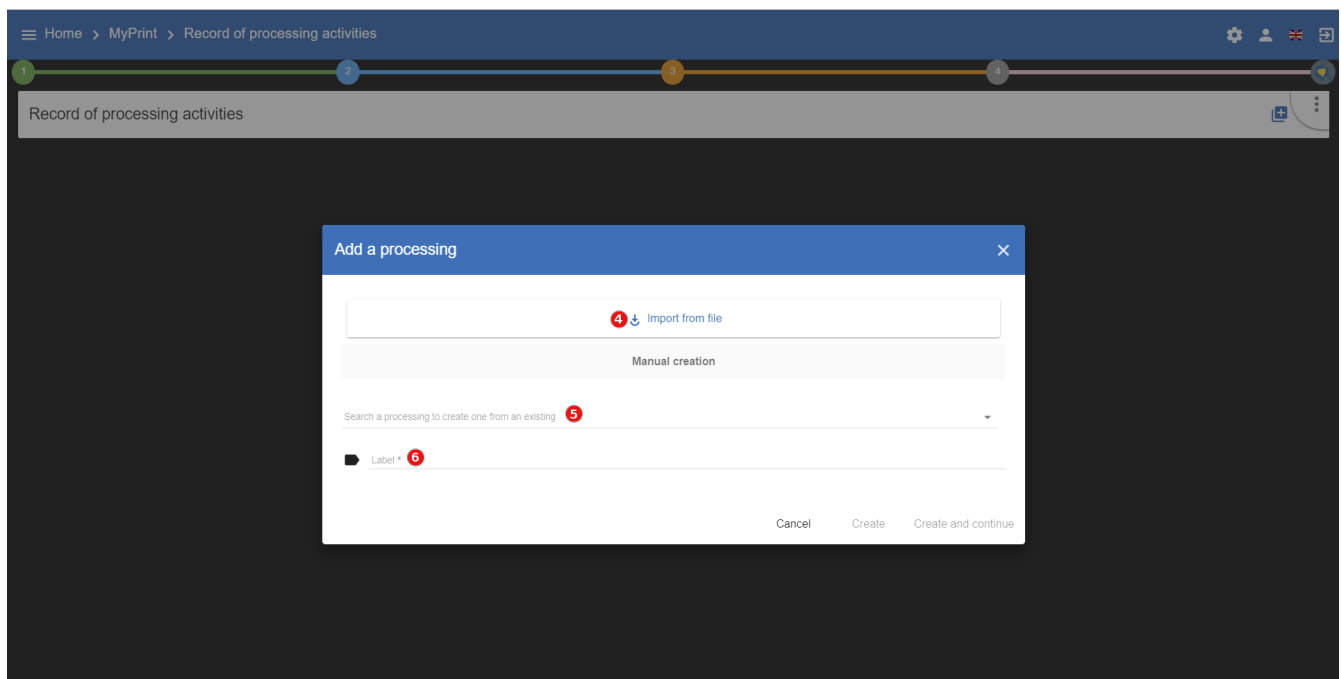
The main goal of this functionality is to help companies to have a list of their processing activities to help to be compliant with GDPR

3. Create the first processing activity

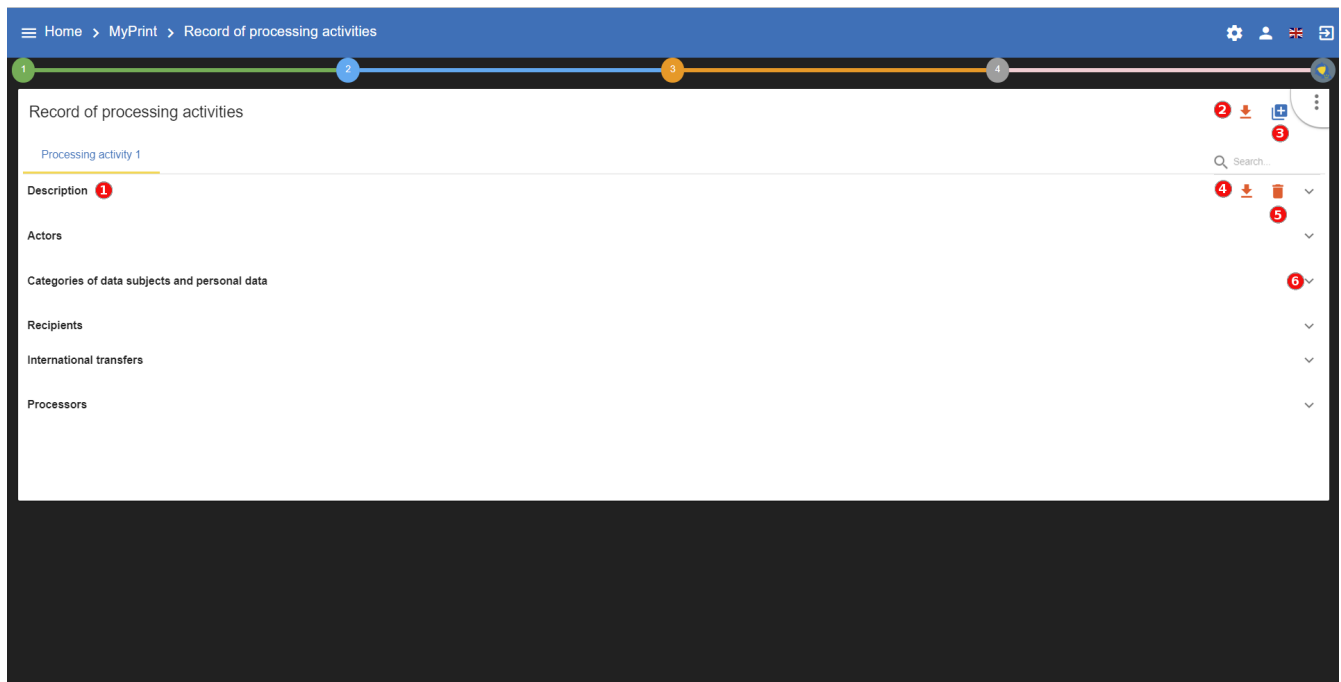


To create a new processing activities you can:

4. **Import** from a JSON file previously exported from MONARC
5. or **Create** it from an existing one
6. if you create one without importing, you have to set a label



The first processing activity is now created. According to the GDPR you can now:



1. Fill six categories (Description, Actors, Categories of data subjects and personal data, Recipients, International transfers, Processors)

You can also :

2. **Download** informations of all the processeceing activities.
3. **Create** a new processing activity.
4. **Download** informations of the selected processeceing activity.
5. **Delete** the selected processing activity.
6. Show or hide a category.

9.1. Description

In this section you have the general information about the selected processing activity:

Record of processing activities

My processing activity

Description

Name	My processing activity ¹
Creation date	2019-08-26 ²
Update date	2019-08-26 ³
Purpose(s)	Le but est de gérer les utilisateurs de MyPrint ⁴
Security measures	Technical security measures - HTTPS - Backup ⁵ Organisational Security measure : - Information Security Policy

Actors

Categories of data subjects and personal data

Recipients

International transfers

Processors

1. **Edit** the name of the selected processecing activity.
2. See the date of creation (automaticly filled by MONARC).
3. See the date of last update (automaticly filled by MONARC).
4. **Fill** the purpose of the processecing activity.
5. **Describe** the main security measures.



To edit a field, you just have to click in the corresponding area to enable the edition and click outside to save your work.

9.2. Actors

In this section you have the actors about the selected processing activity:

Record of processing activities

My processing activity

Description

Actors

Actor	Name	Contact
Controller	MyCompany	1234 boulevard of the L-000 Luxembourg info@mycompany
Data protection officer	My DPO	mydpo@mycompany
Representative	¹	
Joint controllers	My DPO ²	
	MyCompany ⁴	

Categories of data subjects and personal data

Recipients

International transfers

Processors

1. Just click inside to edit and outside to save.
2. Before creating an actor, you can choose one from the existing ones.
3. Delete the corresponding fields of the array.
4. You can **create** several joint controller for one processing activities.

9.3. Categories of data subjects and personal data

In this section you have the actors about the selected processing activity:

Record of processing activities

My processing activity

Description

Actors

Categories of data subjects and personal data 1

Categories of data subject	Categories of personal data	Description	Duration of data retention	Description of retention period
MyPrint users 2	name X 3 firstname X email address X	Those information are necessary to access the service.	2 4 month(s)	The data is stored 2 months after the request to close the space. 5

Recipients

International transfers

Processors

1. **Add** several type of data subjects.
2. **Categories of data subjects**, **Description** and **Description of retention period** are standard editable field.
3. Just type the **category of personal data** and press enter to save it.
4. Set the number for the retention and choose the duration in the drop-down list.
5. **Delete** the corresponding type of data subjects.

9.4. Recipients

In this section you have the recipients about the selected processing activity:

Record of processing activities

My processing activity

Description

Actors

Categories of data subjects and personal data

Recipients 1

Recipient	Recipient type	Description	
MyCompany 2	Internal 3	The data are processed internally. 4	5

International transfers

Processors

1. Add several type of data subjects.
2. Use a recipient from the drop-down list or create a new one.
3. Set the recipient type from the drop-down list.
4. Description is a standard editable field.
5. Delete the corresponding recipient.

9.5. International transfers

In this section you can add an international transfer for the selected processing activity:

Record of processing activities

My processing activity

Description

Actors

Categories of data subjects and personal data

Recipients

International transfers 1

Organisation	Description	Country	Documents	
2				3

Processors

1. Add one more international transfer.
2. Organisation, description, country and documents are standard editable field.

3. **Delete** the corresponding international transfer.

9.6. Processors

In this section you can manage the processors for the selected processing activity:

Record of processing activities

My processing activity


Description

Actors

Categories of data subjects and personal data

Recipients

International transfers

Processors  1

My processor

Name	2 My processor		
Contact	info@myprocessor 1234 boulevard of the L-000 Luxembourg		
Activity(s)	Server management		
Security measures	Backup		

Actors

Actor	Name	Contact
Representative	My DPO 3	mydpo@mycompany 4
Data protection officer		

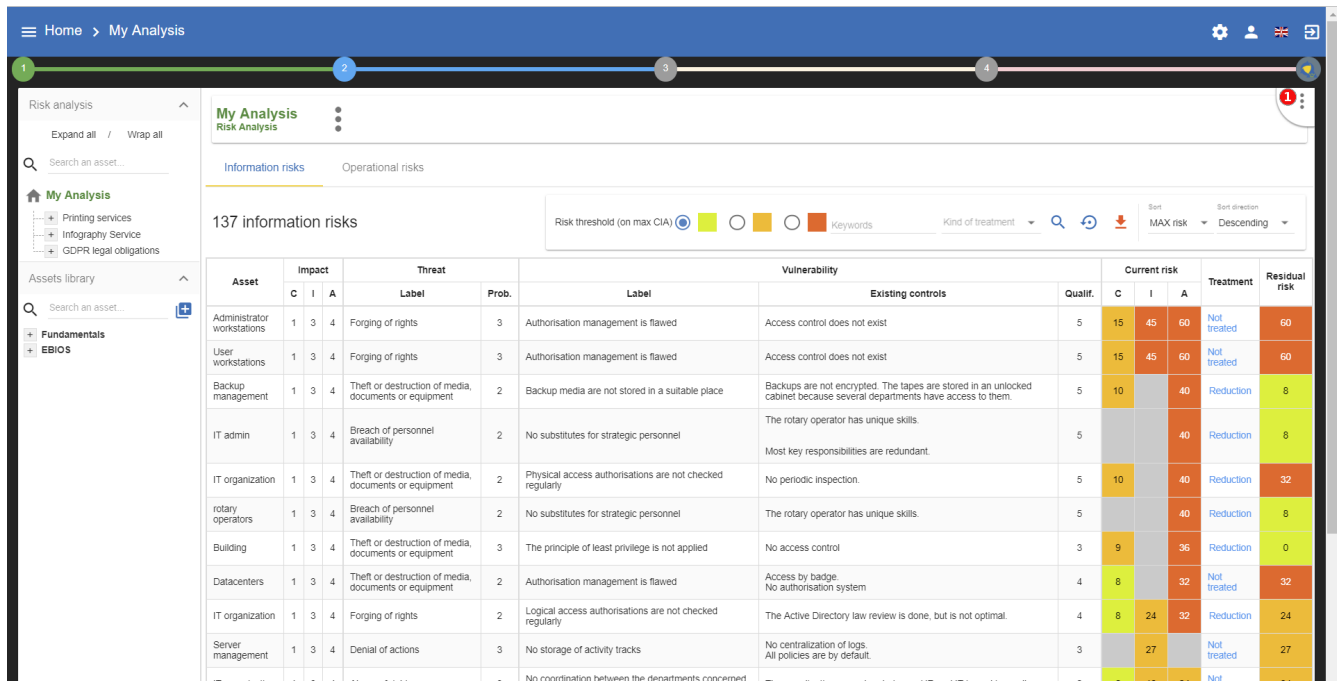
1. **Add** one more processor and feel free to select an existing one or create a new one.
2. **Name**, **Contact**, **Activity** and **security measures** are standard editable field.
3. Use an **actor** from the drop-down list or create a new one.
4. **Delete** the corresponding actor.
5. **Detach** the processor from the selected processing activity.

Chapter 10. 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



My Analysis

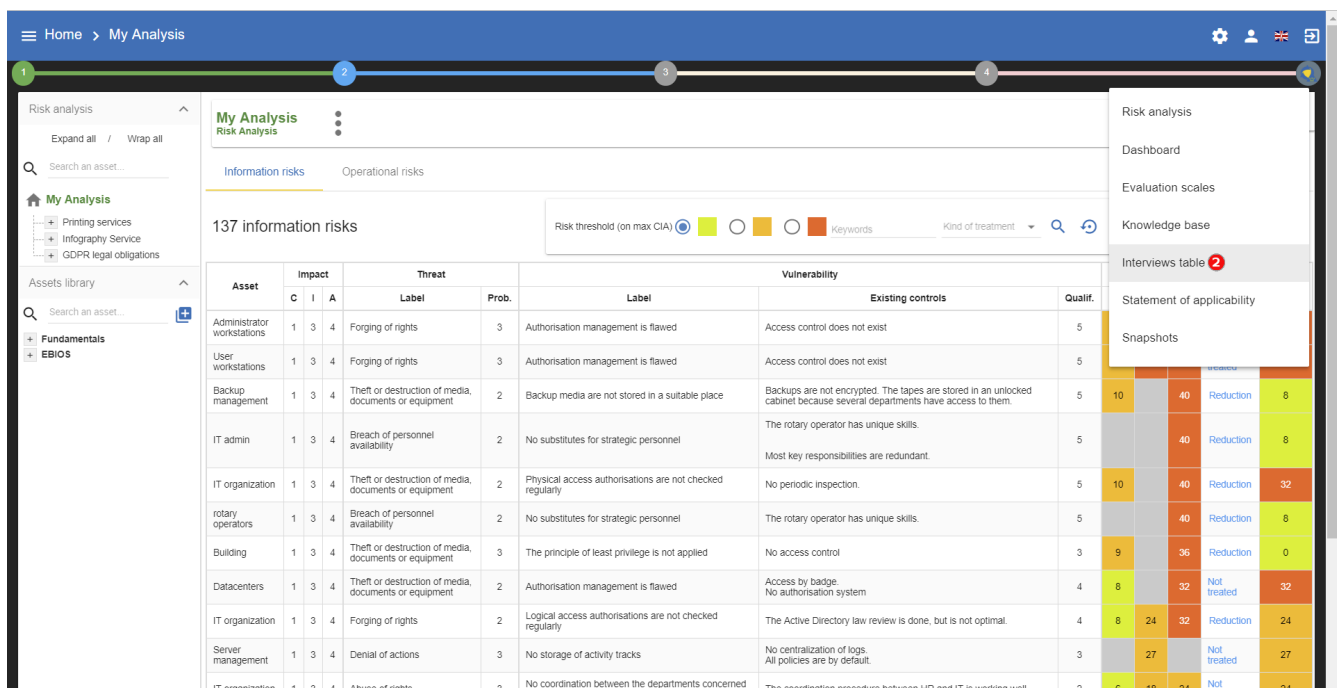
Information risks Operational risks

137 information risks

Risk threshold (on max CIA)  Keywords Kind of treatment Sort MAX risk Sort direction Descending

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Label	Existing controls		C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.		5	10		40	Reduction	8
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.		5			40	Reduction	8
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.		5	10		40	Reduction	32
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.		5			40	Reduction	8
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control		3	9		36	Reduction	0
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system		4	8		32	Not treated	32
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.		4	8	24	32	Reduction	24
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.		3		27		Not treated	27
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	No coordination between the departments concerned	The coordination procedure between IAD and IT is working well		2	6	18	24	Not	24


2. Calling the Management view of Interviews



My Analysis

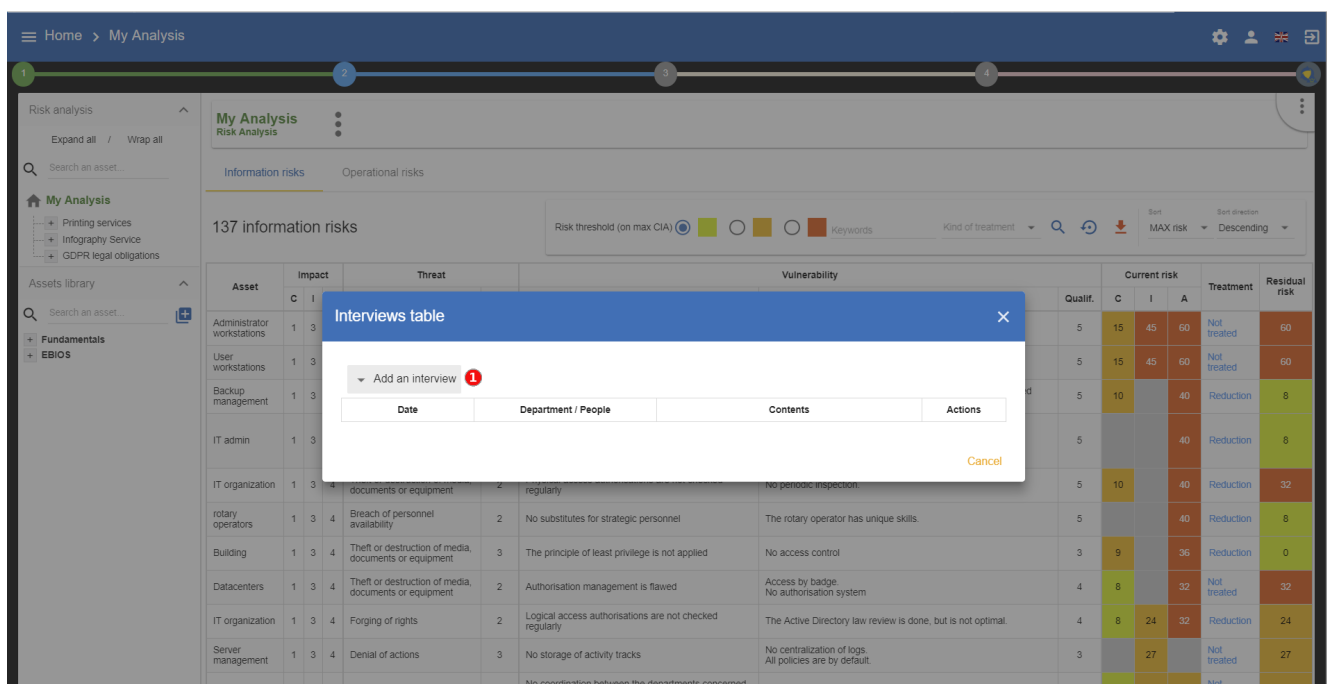
Information risks Operational risks

137 information risks

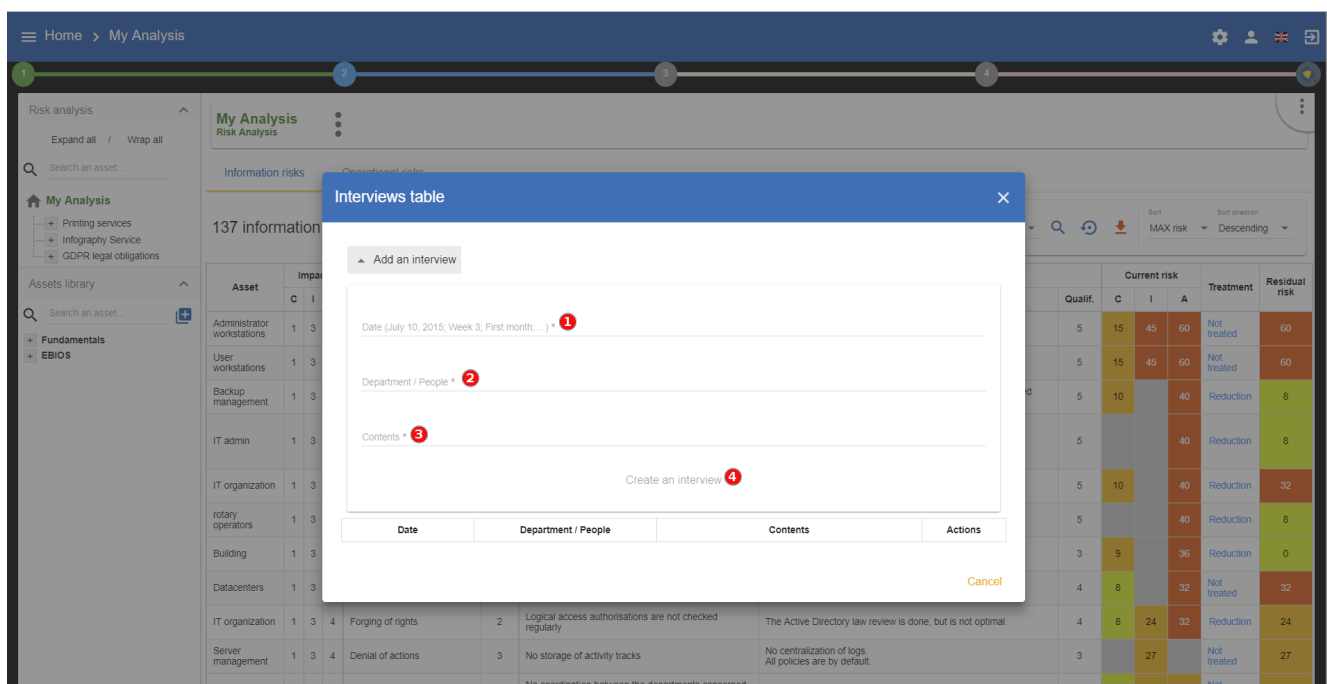
Risk threshold (on max CIA)  Keywords Kind of treatment Sort MAX risk Sort direction Descending

Asset	Impact			Threat	Prob.	Label	Vulnerability		Qualif.	Current risk			Treatment	Residual risk
	C	I	A				Label	Existing controls		C	I	A		
Administrator workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
User workstations	1	3	4	Forging of rights	3	Authorisation management is flawed	Access control does not exist		5	15	45	60	Not treated	60
Backup management	1	3	4	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The tapes are stored in an unlocked cabinet because several departments have access to them.		5	10		40	Reduction	8
IT admin	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills. Most key responsibilities are redundant.		5			40	Reduction	8
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.		5	10		40	Reduction	32
rotary operators	1	3	4	Breach of personnel availability	2	No substitutes for strategic personnel	The rotary operator has unique skills.		5			40	Reduction	8
Building	1	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied	No access control		3	9		36	Reduction	0
Datacenters	1	3	4	Theft or destruction of media, documents or equipment	2	Authorisation management is flawed	Access by badge. No authorisation system		4	8		32	Not treated	32
IT organization	1	3	4	Forging of rights	2	Logical access authorisations are not checked regularly	The Active Directory law review is done, but is not optimal.		4	8	24	32	Reduction	24
Server management	1	3	4	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.		3		27		Not treated	27
IT organization	1	3	4	Theft or destruction of media, documents or equipment	2	No coordination between the departments concerned	The coordination procedure between IAD and IT is working well		2	6	18	24	Not	24

Risk analysis
Dashboard
Evaluation scales
Knowledge base
Interviews table **2**
Statement of applicability
Snapshots



1. Click to encode a new interview



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**

Chapter 11. Snapshots

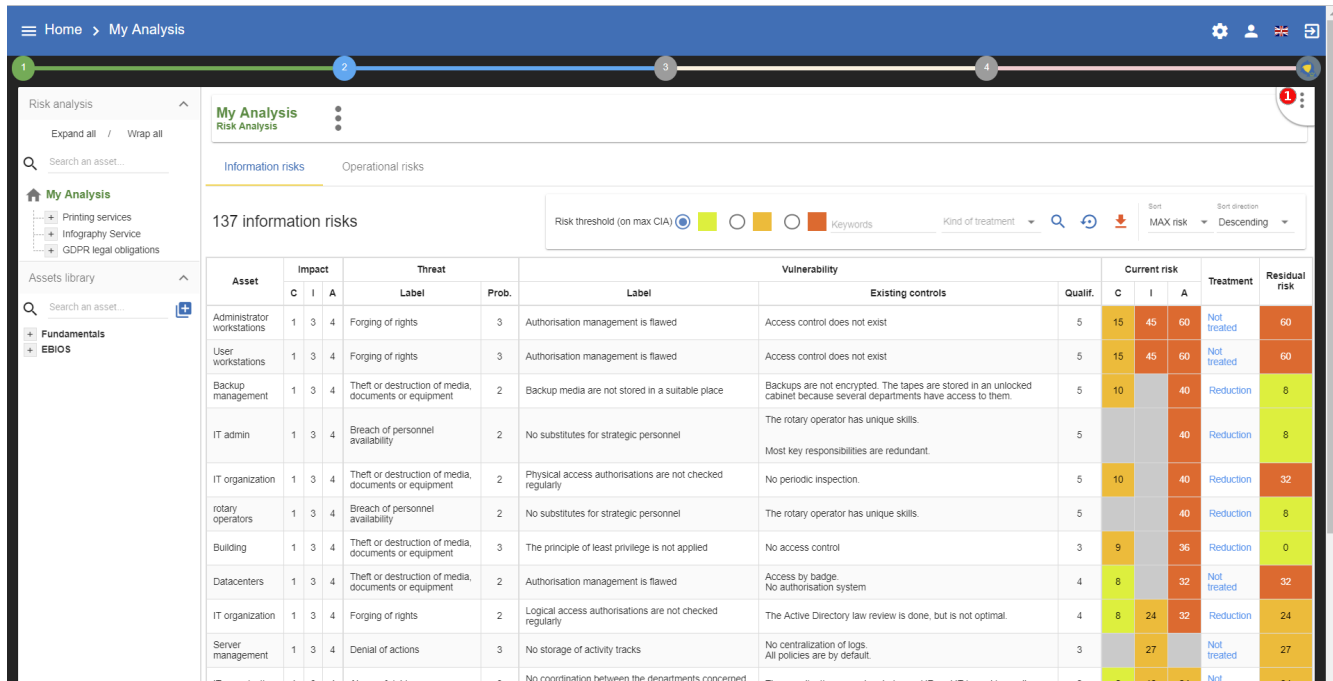
Snapshots allow you to create a full backup for analysis.



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.

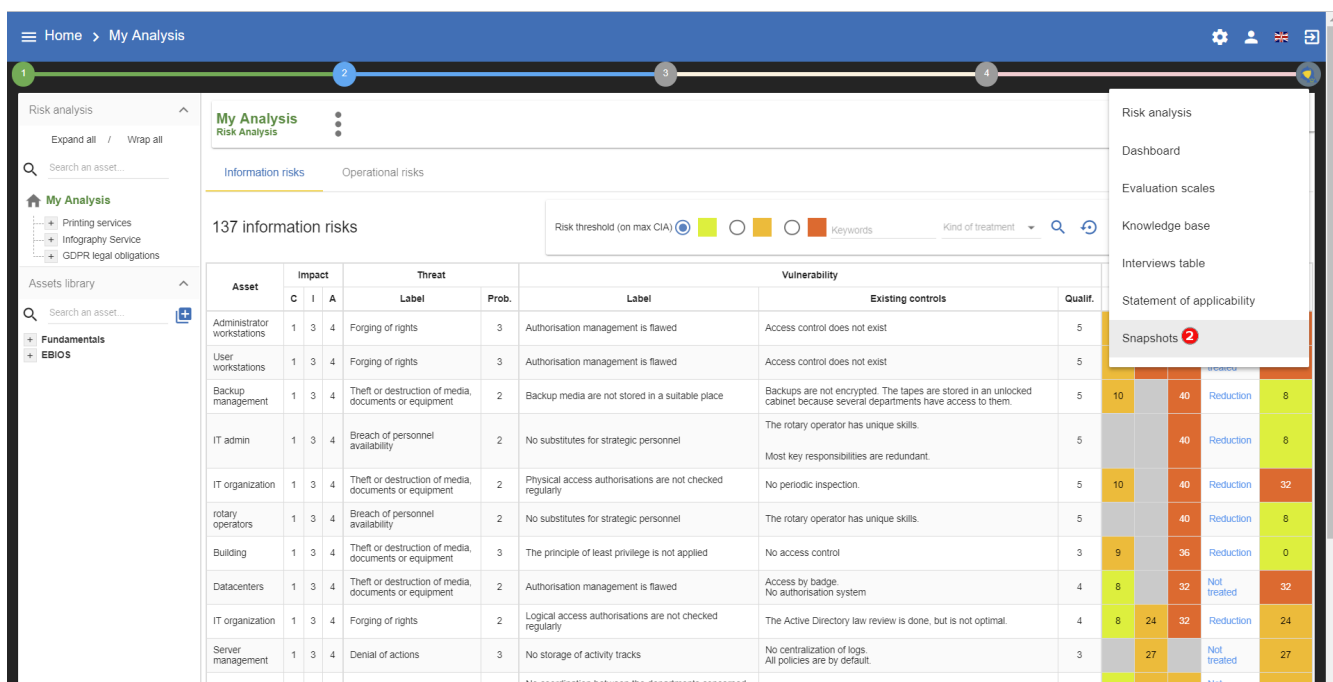
The menu is always accessible from the main view of MONARC:

1. Calling the right contextual menu



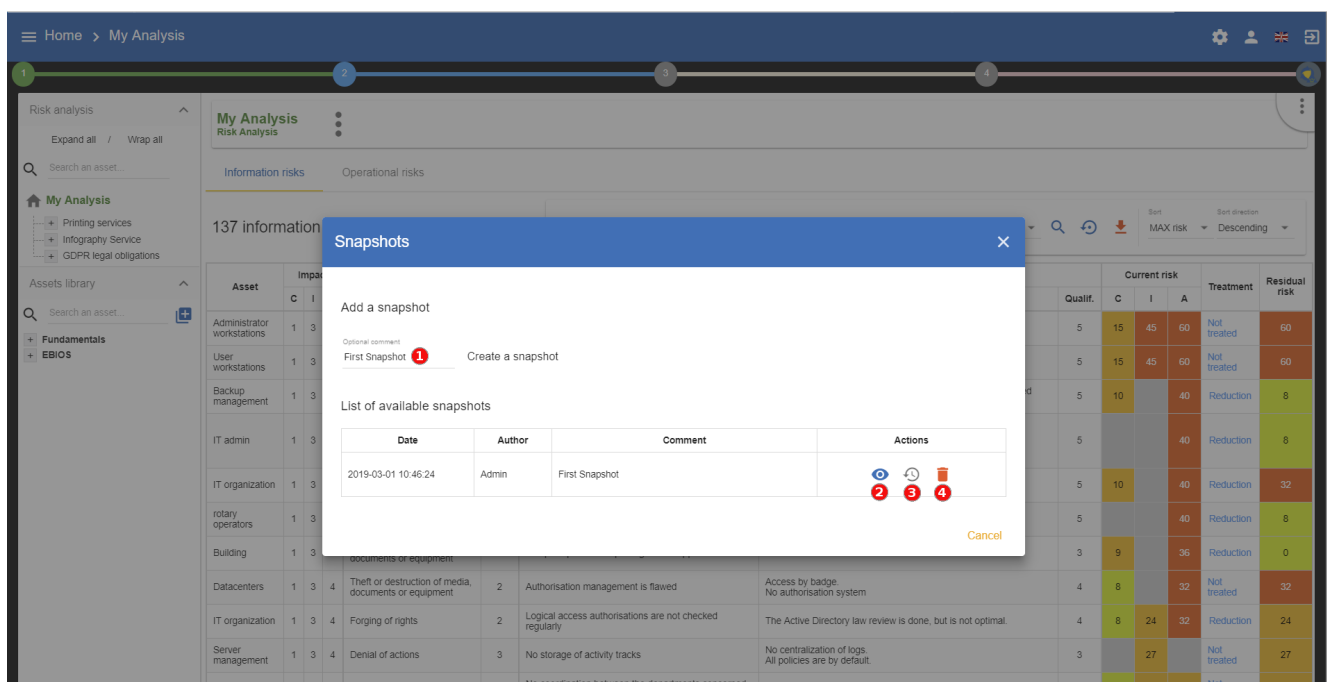
The screenshot shows the MONARC interface with the 'My Analysis' view. The sidebar on the left contains navigation options: 'Risk analysis', 'My Analysis', and 'Assets library'. The main content area displays a table of 137 information risks. The table has columns for Asset, Impact, Threat, Label, Vulnerability, and Current risk. The 'Current risk' column shows a score of 60 for most risks, with some showing a reduction to 8 or 32. A contextual menu is visible in the top right corner, showing options like 'Risk analysis', 'Dashboard', 'Evaluation scales', 'Knowledge base', 'Interviews table', 'Statement of applicability', and 'Snapshots'.

2. Calling the Management view of Snapshot



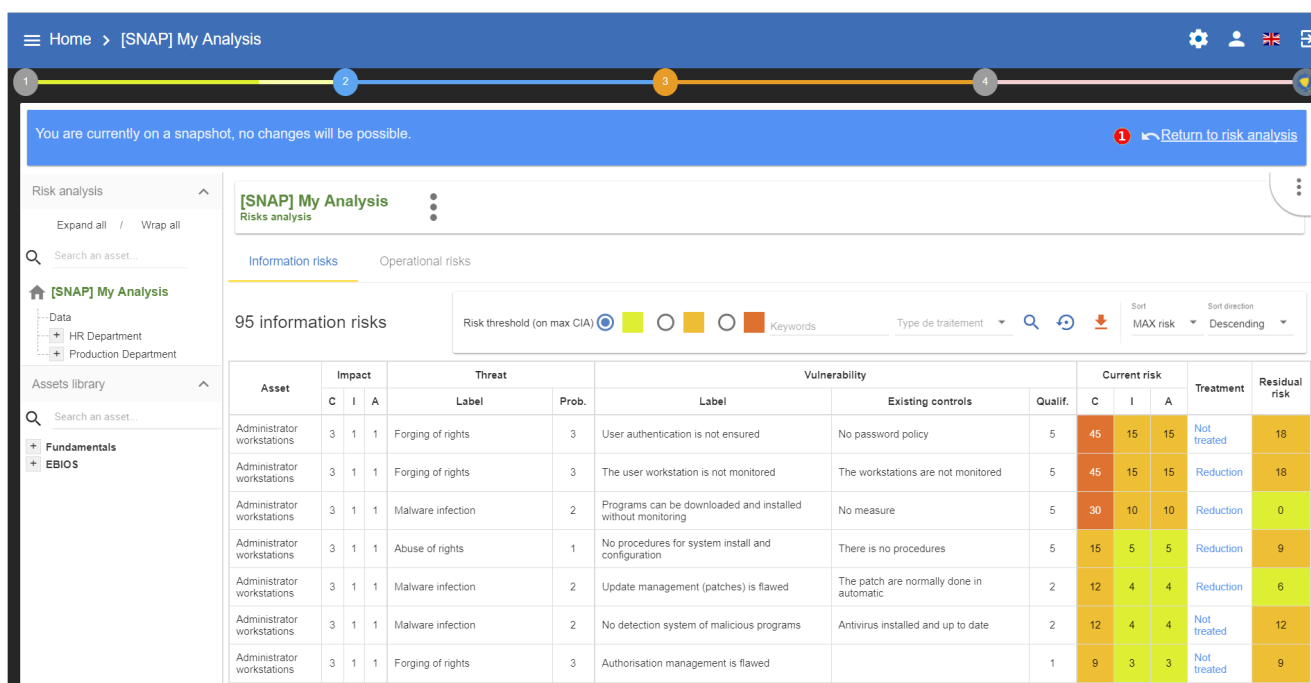
The screenshot shows the MONARC interface with the 'My Analysis' view. The sidebar on the left contains navigation options: 'Risk analysis', 'My Analysis', and 'Assets library'. The main content area displays a table of 137 information risks. The table has columns for Asset, Impact, Threat, Label, Vulnerability, and Current risk. The 'Current risk' column shows a score of 60 for most risks, with some showing a reduction to 8 or 32. A contextual menu is visible in the top right corner, showing options like 'Risk analysis', 'Dashboard', 'Evaluation scales', 'Knowledge base', 'Interviews table', 'Statement of applicability', and 'Snapshots'.

The following pop-up appears:



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:



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

Chapter 12. Managing the Implementation Treatment Plan

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

The screenshot shows the MONARC Risk Analysis interface. The top navigation bar includes 'Home > My Analysis'. The left sidebar contains 'Risk analysis', 'My Analysis', and 'Assets library'. The main content area displays '84 information risks' with a table of risk details. A dropdown menu is open, showing 'Implementation and monitoring' with a checkbox for 'Management of the implementation of the risk treatment plan'.

Asset	Impact			Threat	Prob.	Vulnerability			Qualif.	Current risk			Treatment	Residual risk
	C	I	A			Label	Existing controls	C		I	A			
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	Forging of rights	3	Authorisation management is flawed	No procedure	4	36	12	12	Reduction	9	
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	Not treated	15	
Administrator workstations	3	1	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	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	User authentication is not ensured	No password policy	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	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.

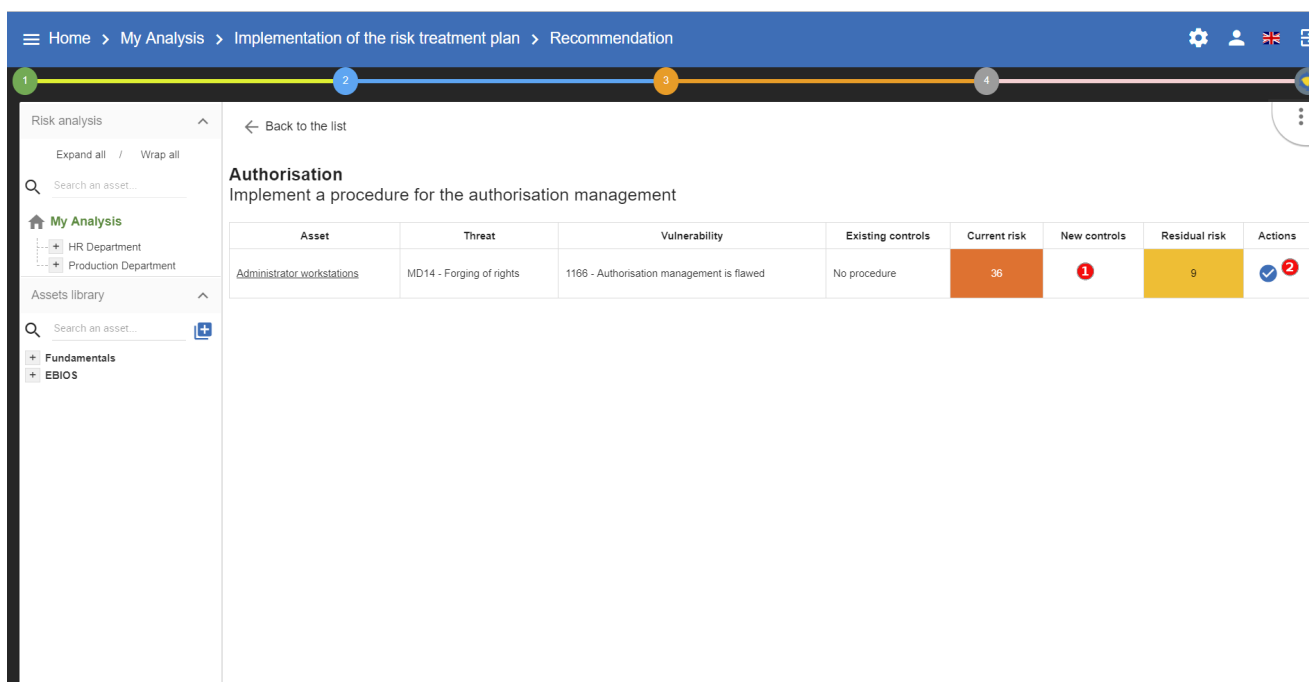
The screenshot shows the 'Implementation of the risk treatment plan' view. It includes a table with columns for Recommendation, Imp., Comment, Manager, Deadline, Status, and Actions. The table lists several recommendations for implementation, such as 'Authorisation', 'Monitoring', 'Program management', 'Administrator right', and 'Patch management'.

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

1. This is a **recommandation** 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.



Home > My Analysis > Implementation of the risk treatment plan > Recommendation

Risk analysis

Expand all / Wrap all

Search an asset...

My Analysis

- HR Department
- Production Department

Assets library

Search an asset...


Fundamentals

EBIOS

Back to the list

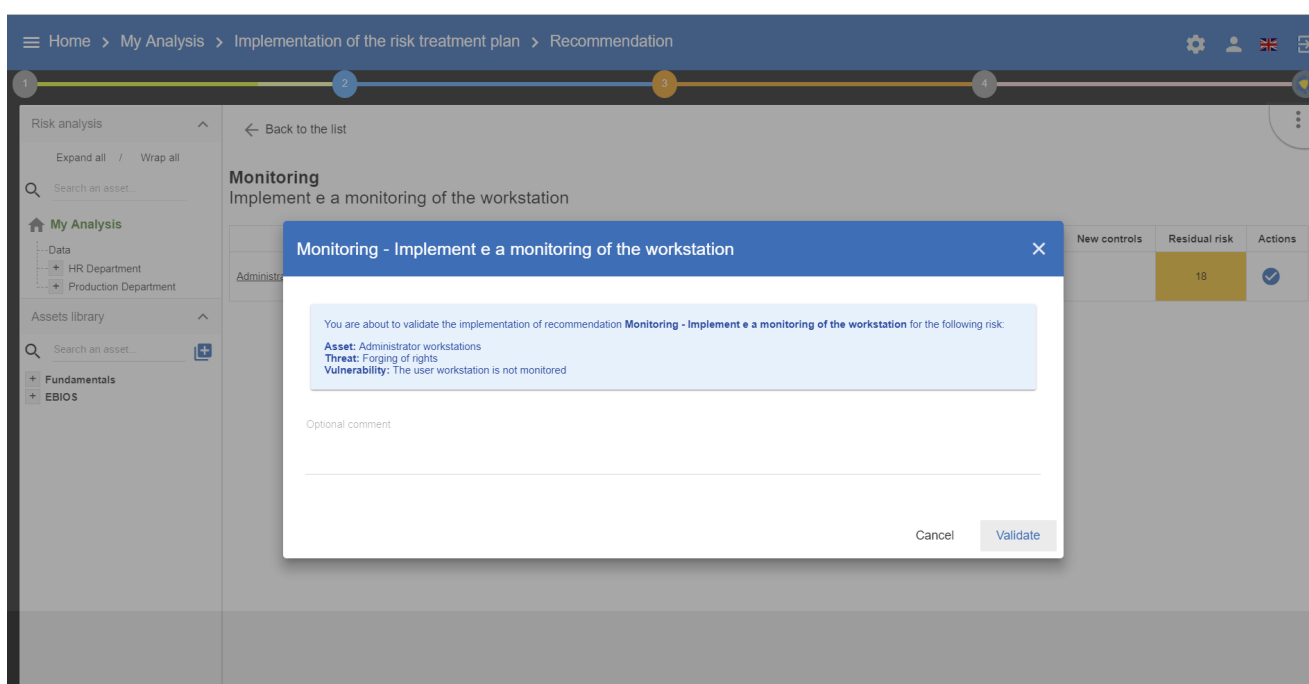
Authorisation

Implement a procedure for the authorisation management

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	36	1	9	 2

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 



Home > My Analysis > Implementation of the risk treatment plan > Recommendation

Risk analysis

Expand all / Wrap all

Search an asset...

My Analysis

- Data
- HR Department
- Production Department

Assets library

Search an asset...


Fundamentals

EBIOS

Back to the list

Monitoring

Implement e a monitoring of the workstation

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	36	1	9	 2

Monitoring - Implement e a monitoring of the workstation

You are about to validate the implementation of recommendation **Monitoring - Implement e a monitoring of the workstation** for the following risk:

Asset: Administrator workstations
Threat: Forging of rights
Vulnerability: The user workstation is not monitored

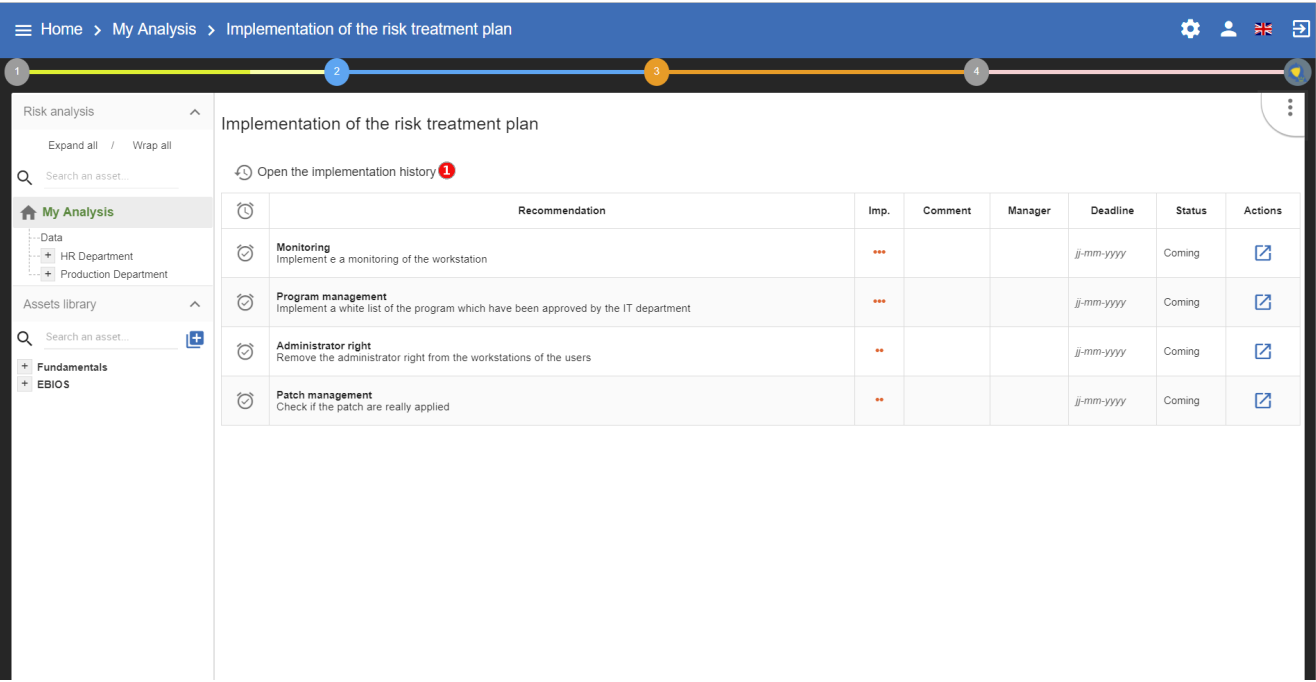
Optional comment

Cancel Validate

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:



1. Click to view past recommendations

