User Guide

NC3 Luxembourg

Version 2026-08-18

Table of Contents

1. Introduction . . . 2
    1.1. Purpose . . . 2
    1.2. Other documents . . . 2
    1.3. Syntax used in the document . . . 2
    1.4. Syntax used in MONARC . . . 2
2. Home Page . . . 3
    2.1. Home page . . . 3
    2.2. Creating a Risk Analysis . . . 4
    2.3. Main risk analysis view . . . 6
3. Client Environment Administration . . . 8
    3.1. Administration . . . 8
4. Analysis Management . . . 25
    4.1. Risk analysis management . . . 25
    4.2. Method steps call . . . 29
    4.3. Risks management . . . 31
    4.4. Library . . . 32
    4.5. Information Risks . . . 41
    4.6. Operational Risks . . . 52
5. Evaluation Scales . . . 59
    5.1. Information risks . . . 60
    5.2. Operational risk scales . . . 63
    5.3. Compliance . . . 66
6. Management of Knowledge Base . . . 70
7. Selecting assets separately or as a group . . . 73
    7.1. Type of assets . . . 73
    7.2. Threats . . . 73
    7.3. Vulnerabilities . . . 74
    7.4. Referentials . . . 74
    7.5. Information Risks . . . 75
    7.6. Tags (Operational Risks) . . . 77
    7.7. Operational Risks . . . 77
    7.8. Risk Sources . . . 78
    7.9. Recommendations Sets . . . 79
8. Statement of applicability . . . 81
9. Dashboard . . . 84
10. Record of processing activities . . . 86
11. How to record a processing activity? . . . 87
    11.1. Description . . . 88

11.2. Actors . . . 89
11.3. Categories of data subjects and personal data . . . 90
11.4. Recipients . . . 90
11.5. International transfers . . . 91
11.6. Processors . . . 92
12. Interviews . . . 93
13. Snapshots . . . 96
14. Managing the Implementation Treatment Plan . . . 99
15. Global Dashboard . . . 103

New in MONARC v2.14.1

- **ISO 27005:2022 adaptations:** risk sources, reassessment triggers and schedules, review governance, residual-risk approval, risk history, and role-based risks management. See the separate companion document: HTML or PDF.
- **PDF report generation:** select PDF when generating a deliverable. See Generate a PDF report and issue #615.
- **Blank Analysis:** create a completely empty analysis without Knowledge Base or Assets library data. See Creating a Risk Analysis and issue #324.
- **CyFun referentials:** use the CyFun Basic, Important, and Essential 2025 referentials with ISO 27002 mappings. See New in MONARC v2.14.1: CyFun referentials and issue #616.

Chapter 1. Introduction

1.1. Purpose

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

1.2. Other documents

- **Quick Start**: Provides a quick start about MONARC.
- **Method Guide**: Provides the complete documentation of the method.
- **Technical Guide**: Provides the complete technical documentation of the tool.

1.3. Syntax used in the document

All numbers in white on an orange 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

The three-dot menu icon brings up the menu items.

Create/add something in context (assets, recommendations, etc.).

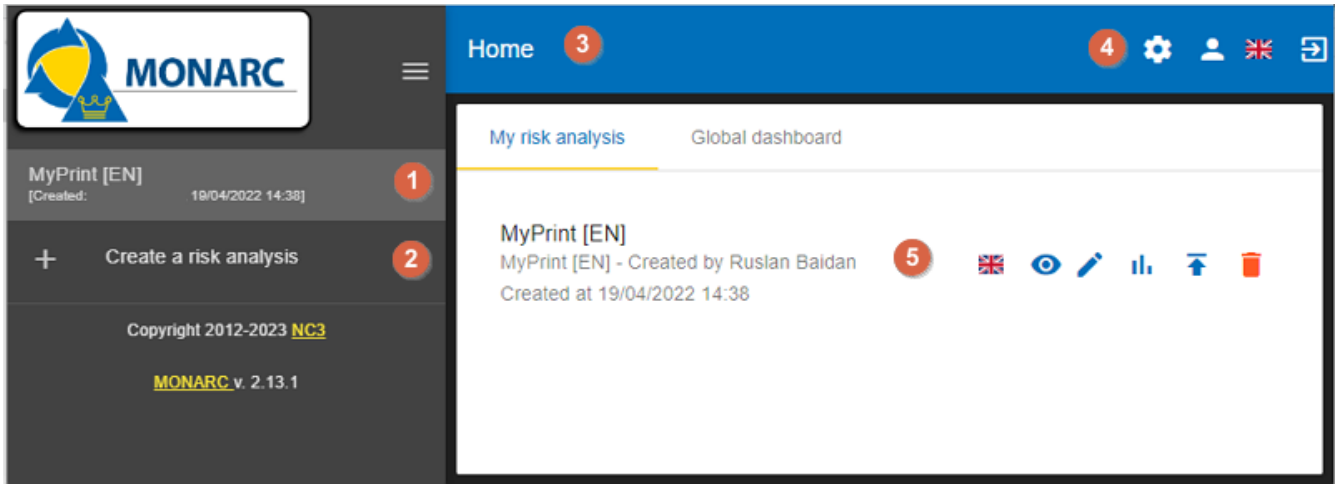
Most fields of MONARC display additional information when the pointer stays unmoved for some time.

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.

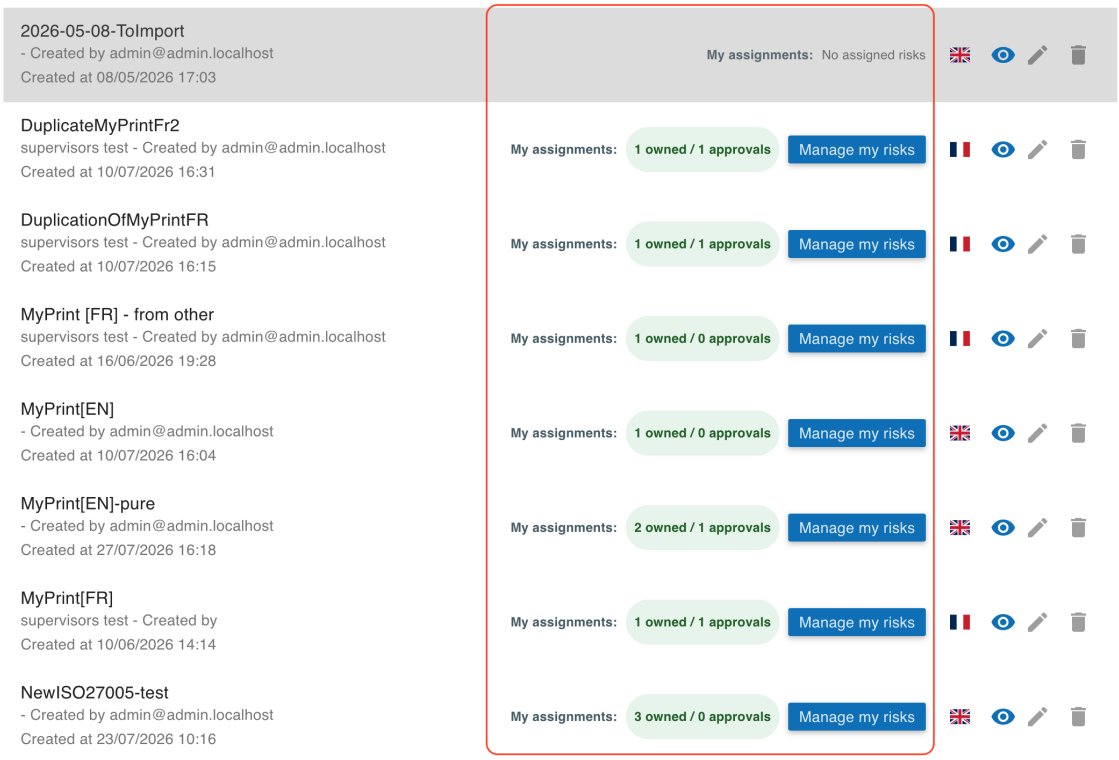


On the Home page, the following main areas and functionalities can be found:

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

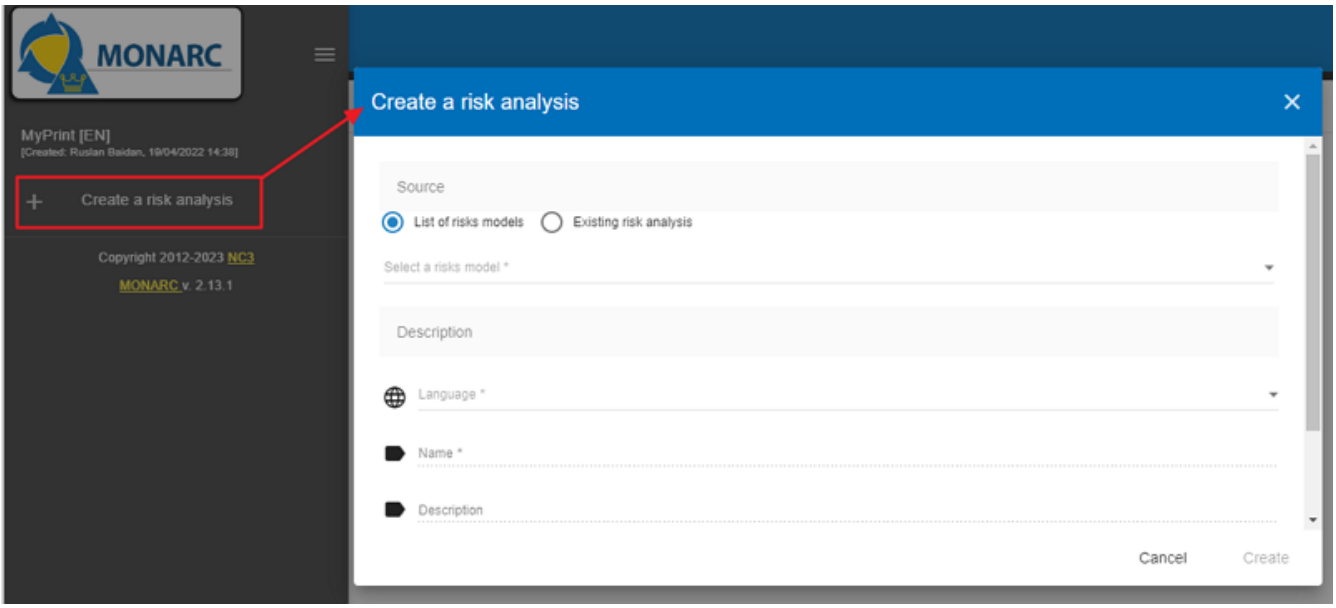
New in MONARC v2.14.1

When the current user is linked to an active analysis supervisor, the `My risk analysis` list can also display a `My assignments` indicator with owned and approval counts. If at least one assigned risk exists, the `Manage my risks` button opens the dedicated `Risks management` view directly from the home page.

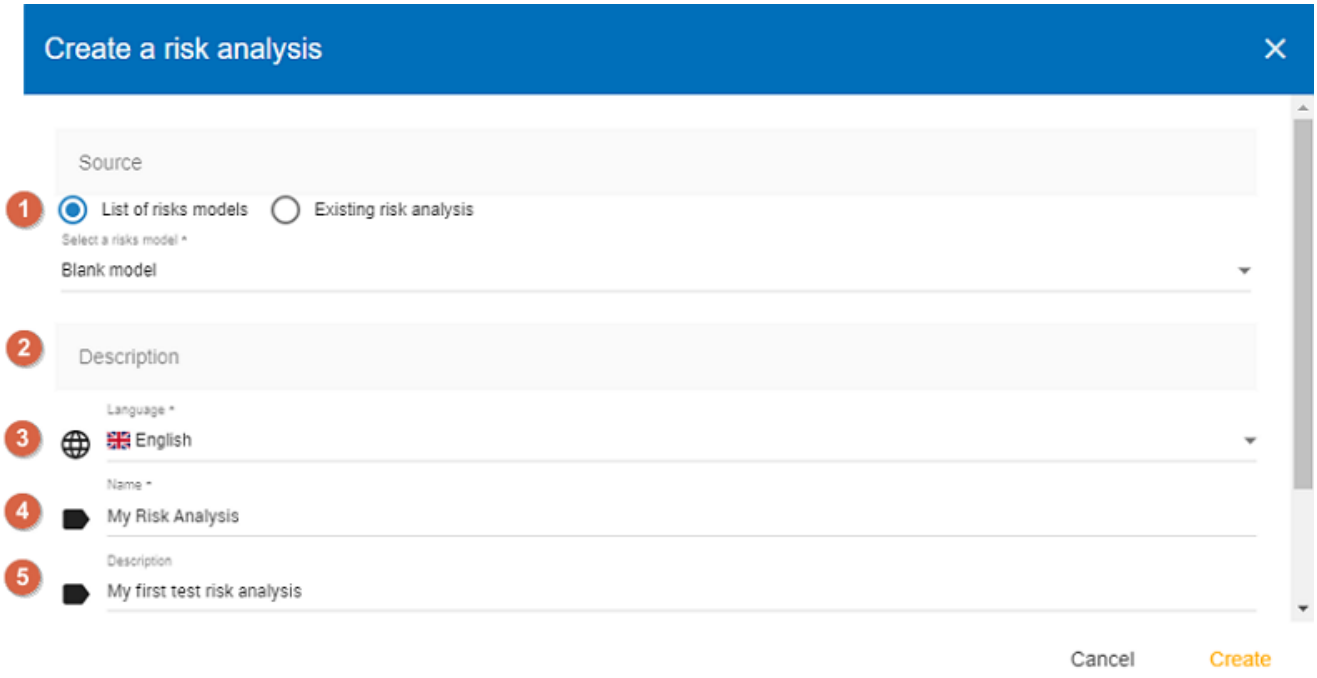


2.2. Creating a Risk Analysis

After clicking on `Create a risk analysis`,



the following pop-up appears:



1. **Source**: By default, the creation of a risk analysis is based on an existing model. There are two choices for this:
    1. `List of risks models`: This option proposes available models in the knowledge bases. It has at least two choices, `Modelling NC3`, and the `Blank model`. Modelling NC3 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.

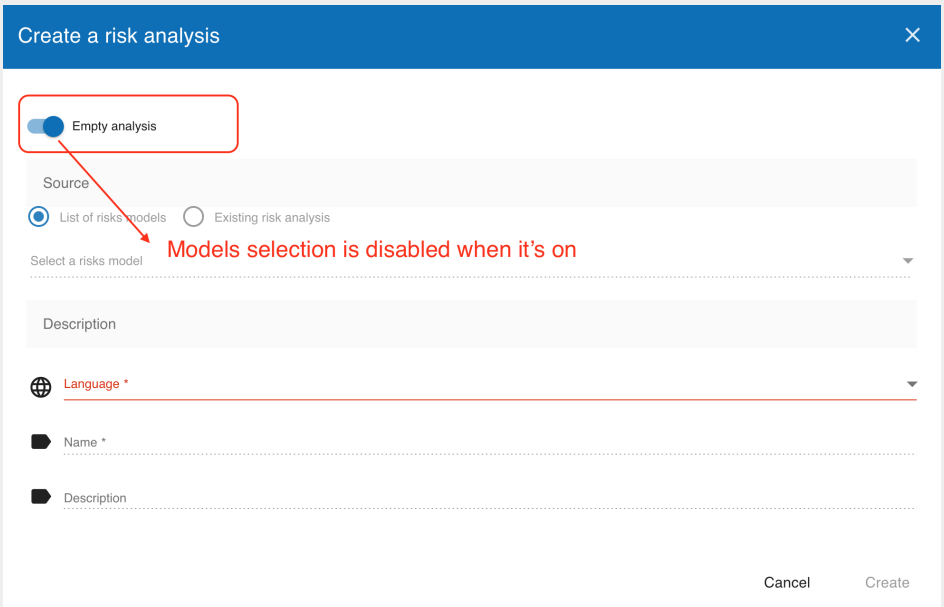
        ```
        The Blank model is empty. This template is typically used temporarily as a
        Sandbox to test the contents of an import file, for example.
        ```

    2. `Existing analysis`: By choosing this radio button, you can duplicate the risk analysis of your choice present in your environment.
2. **Description**: Give a meaningful description of your risk analysis.
3. **Language**: From the dropdown menu, choose a preferred language you want to use for your risk analysis (French, English, German, or Dutch).
4. **Name**: Give a name to your risk analysis.
5. **Description**: An optional field, which allows you to describe your analysis in more detail.

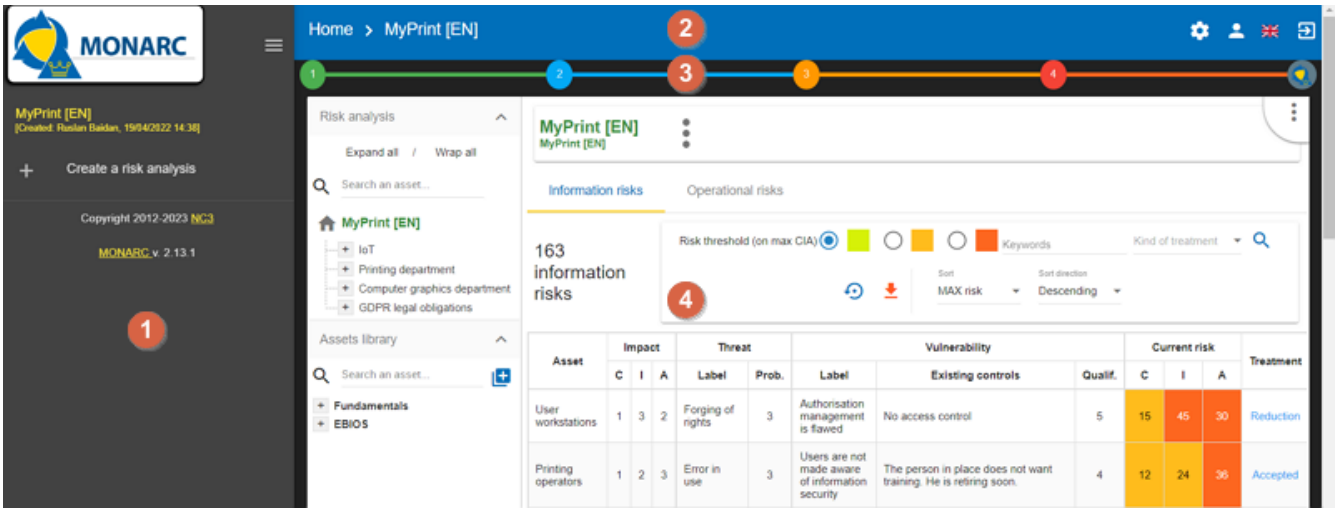
New in MONARC v2.14.1

Available from MONARC v2.14.1, `Empty analysis` lets you start without a preconfigured model. Enable the switch at the top of the creation window. This disables model and source selection, clears selected referentials, and lets you select any active system language.

Creating a risk analysis now offers the `Empty analysis` option. It creates a completely empty risk analysis, without data in the Knowledge Base or Assets library. MONARC still creates the evaluation-scale baseline required to configure the analysis. Use this option when you want to build the scope and knowledge base from scratch. See issue #324 for the associated release item.



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: An administrator can create, modify, and delete users.

> An administrator does not have access rights to the risk analysis (but he can give them).

- Users: The users have access rights to risk analysis.

In the top right-hand corner of the Navigation bar, the follwing isons can be seen:

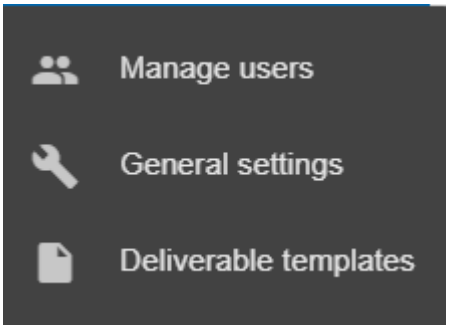
1. Administration (Accessible only for administrator users)
   - Manage users (see Manage users)
   - General settings (see [Organization])
   - Deliverable templates (see Deliverable templates)
2. User account (see User account)
3. Interface language (see Interface language)
4. Logout

3.1. Administration

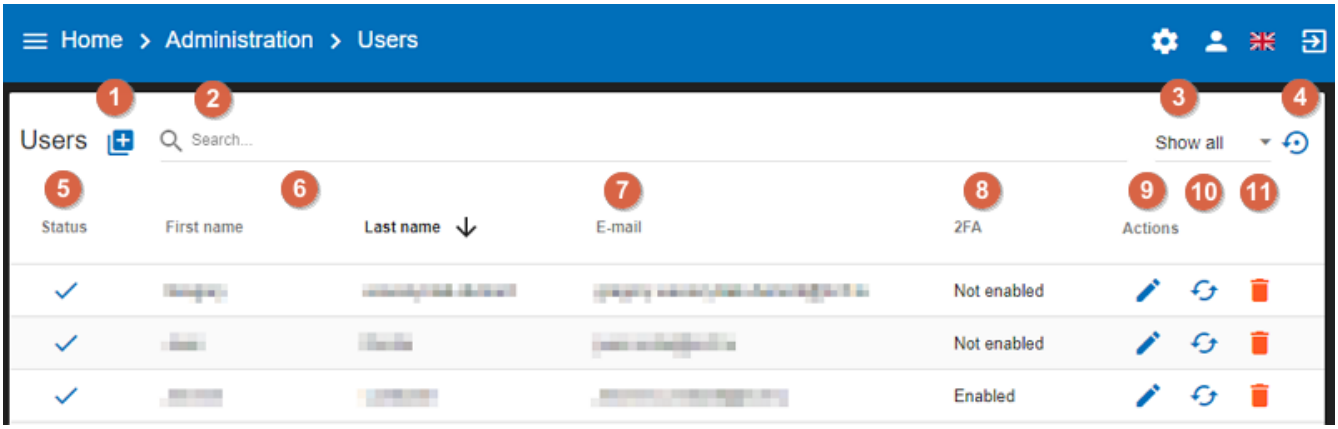
3.1.1. Manage users

List of users

By clicking on the gear icon in the top right-hand corner, the following menu appears:



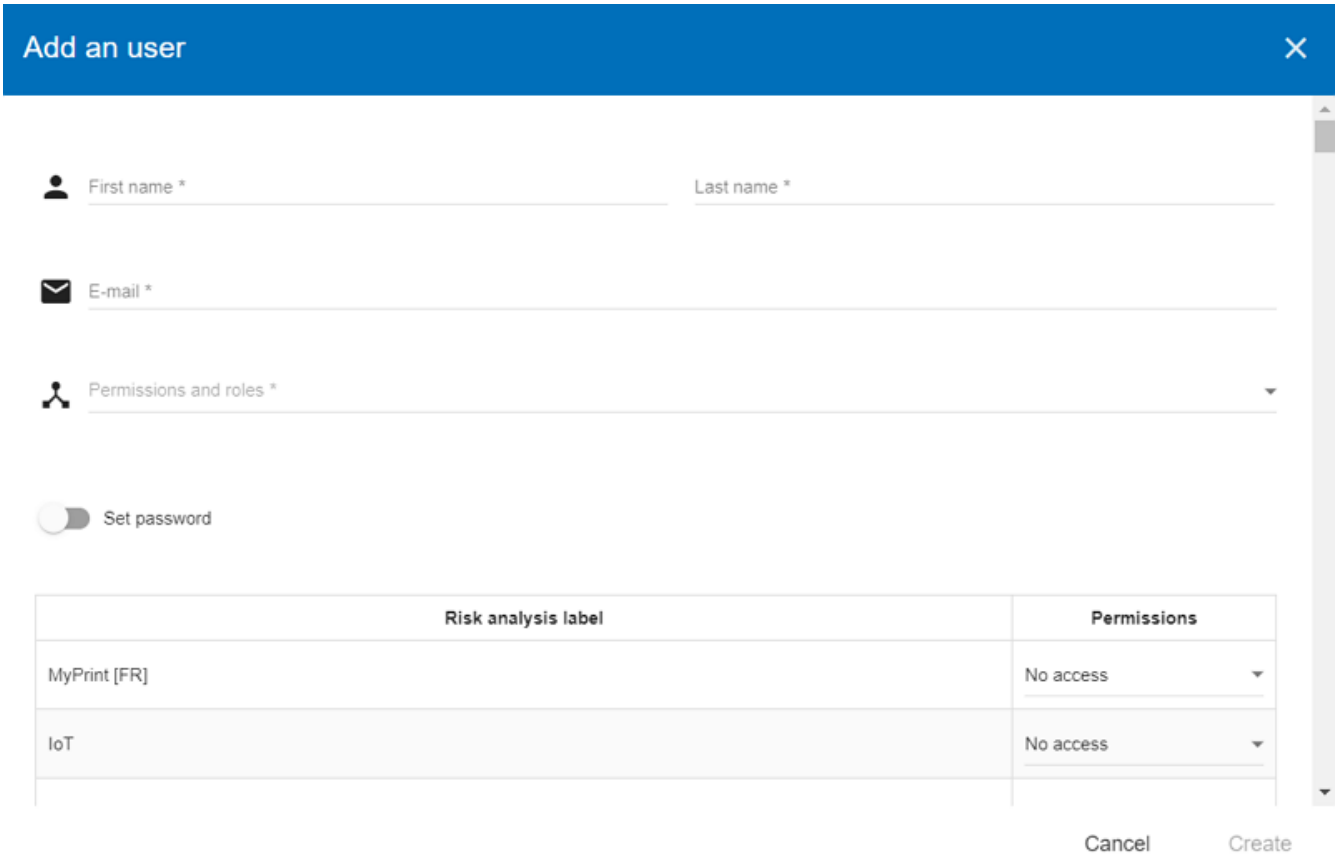
If you click on the ‘Manage users’ option, the Users screen appears:



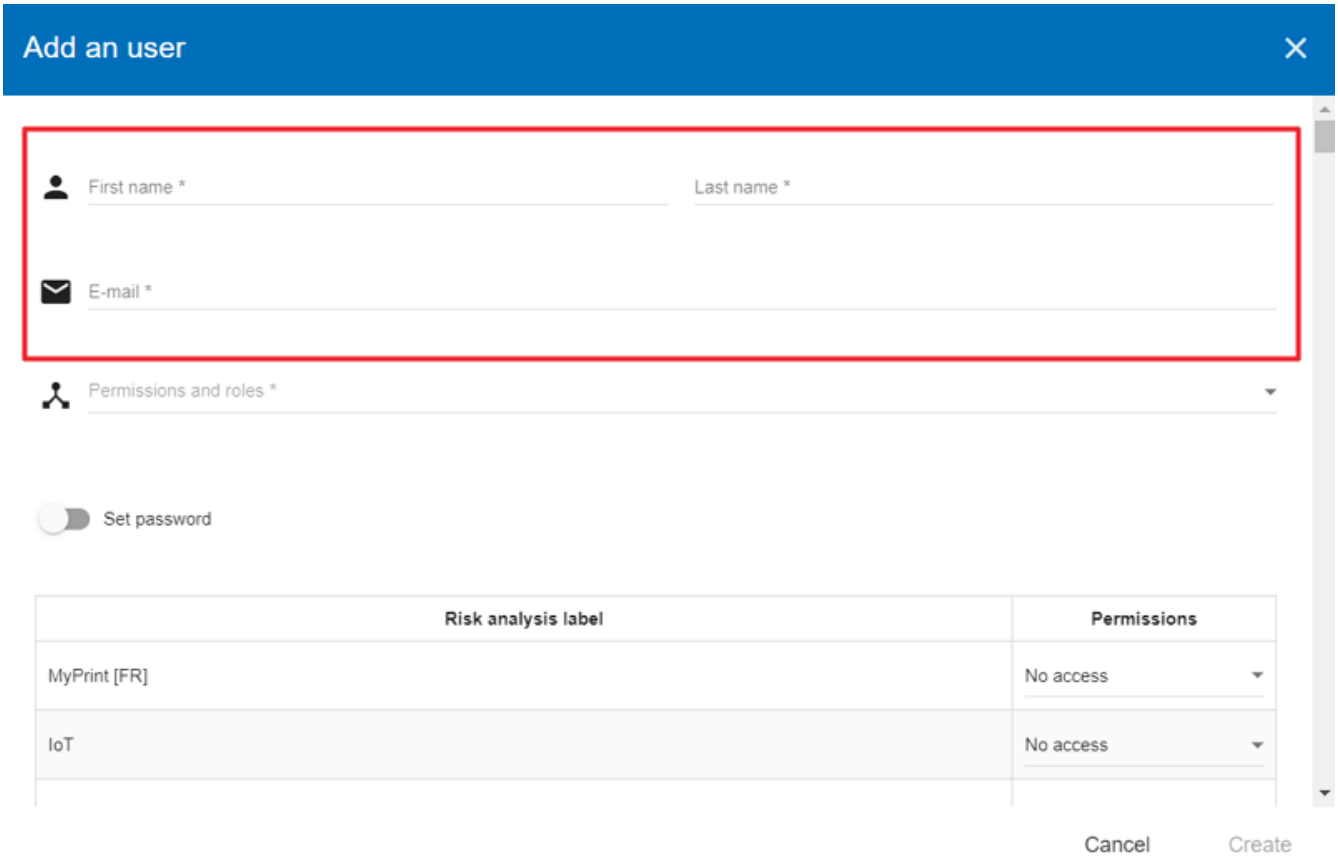
1. **Users**: You can create a user or administrator.
2. **Search**: You can search among the users/administrators (the list will automatically update).
3. **Filter**: you can filter the list, there are three options: Show all, Show inactive only, Show active only.
4. **Undo**: You can go back to the previously filtered list.
5. **Status**: This column shows the status of the users (active: chackmark, inactive cross).
6. **First and Last name** of the users.
7. **E-mail**: the email addresses of the users.
8. **2FA**: this column shows whether the user enabled or not enabled two factor authentication.
9. **Edit**: by clicking on a pencil icon, you may edit the chosen user's data in the system.
10. **Reset password**: by clicking on the circular two-arrows icon, you may reset the password of the chosen user.
11. **Delete**: by clicking on the trash bin icon, you can delete the schosen user.

Add a user

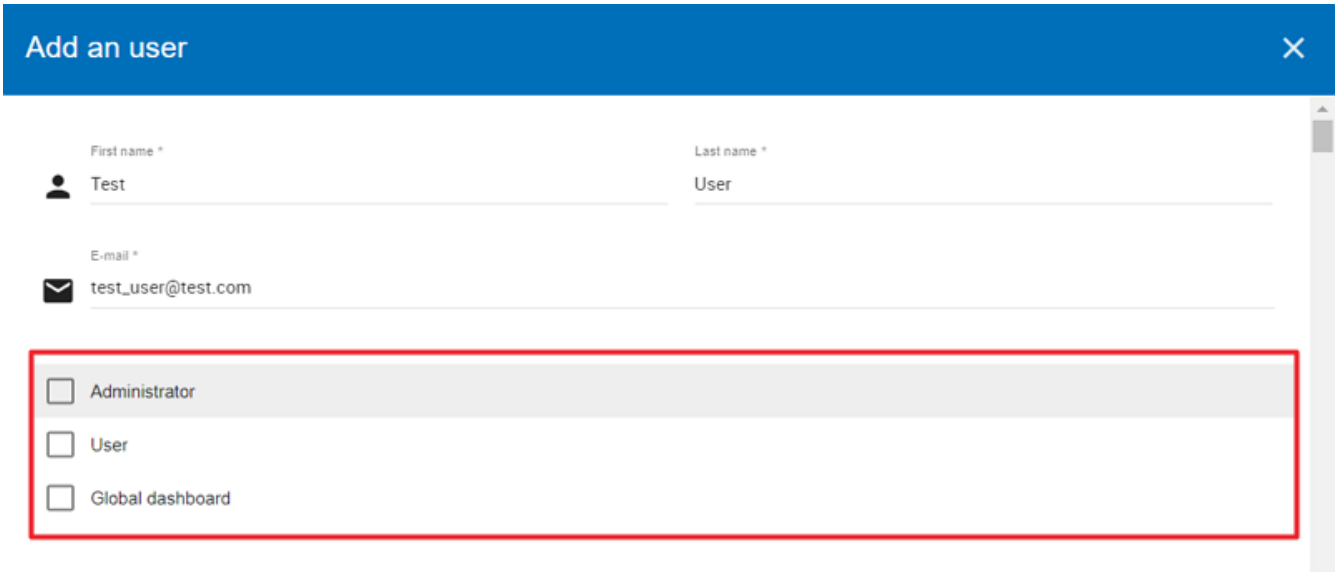
If you click on the + icon in the top left-hand corner, the following screen appears:



Fill in the ‘First name’ and ‘Last name’ fields, and add an e-mail address.

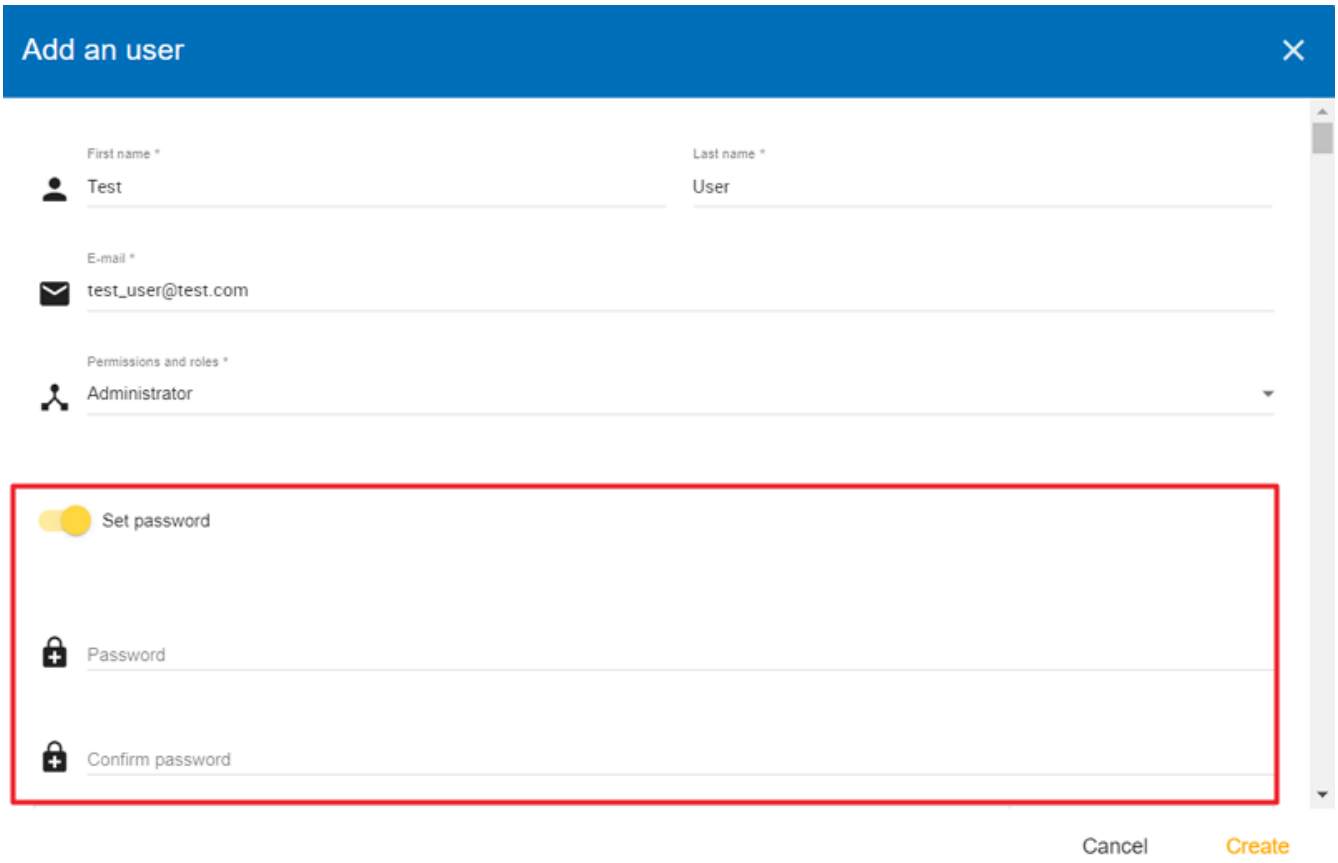


Then, click on the ‘Permissions and Roles’ option to change the screen, where you can choose from three options: Administrator, User, or Global dashboard.

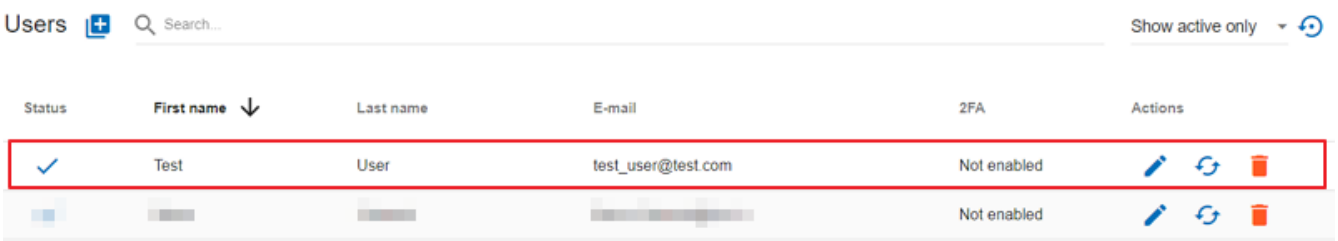


Set a password

As the next step, set the password for the new user by clicking on the toggle to activate it:



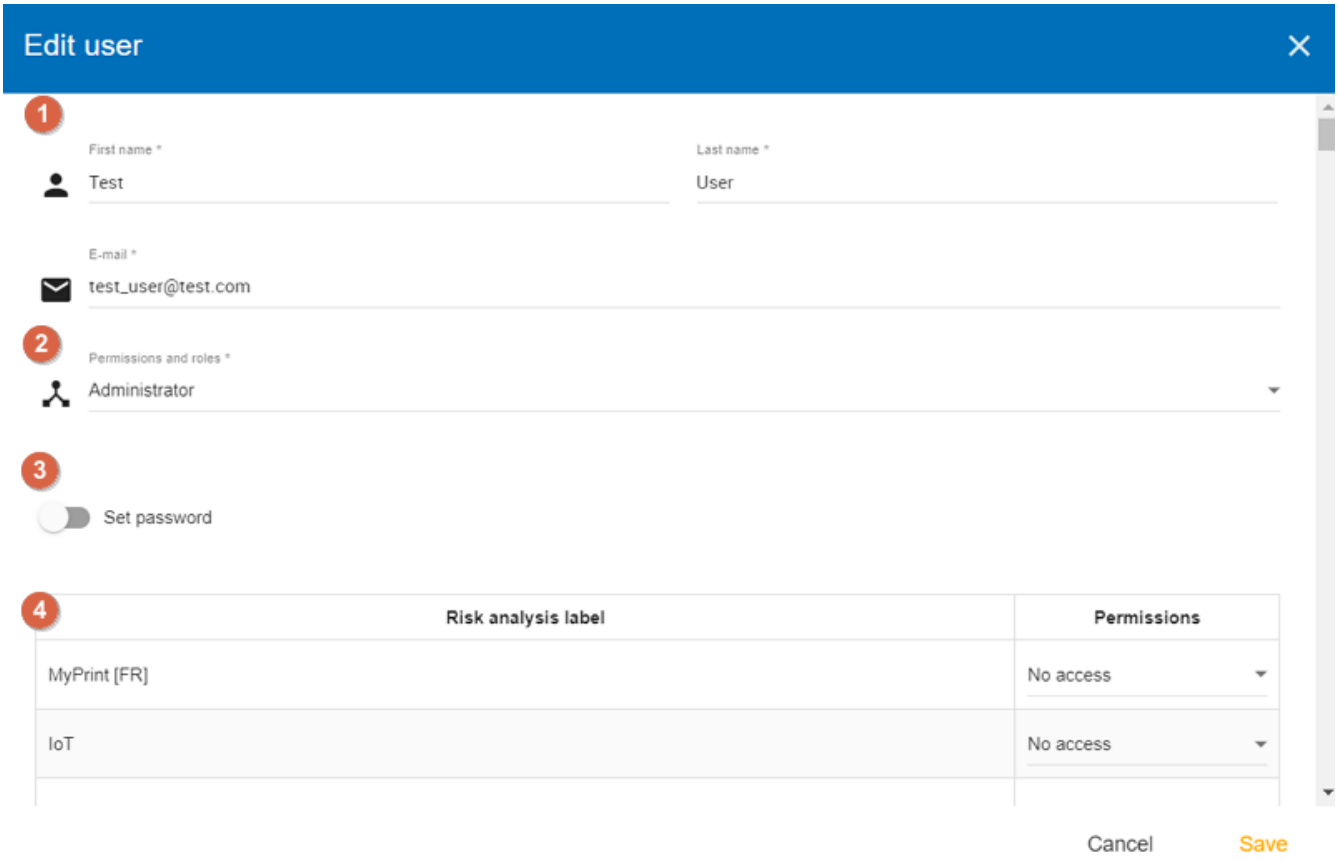
Once the password field is populated, click on the Create button (in the lower right-hand corner). The newly-created user becomes visible in the list of users.



User rights and information

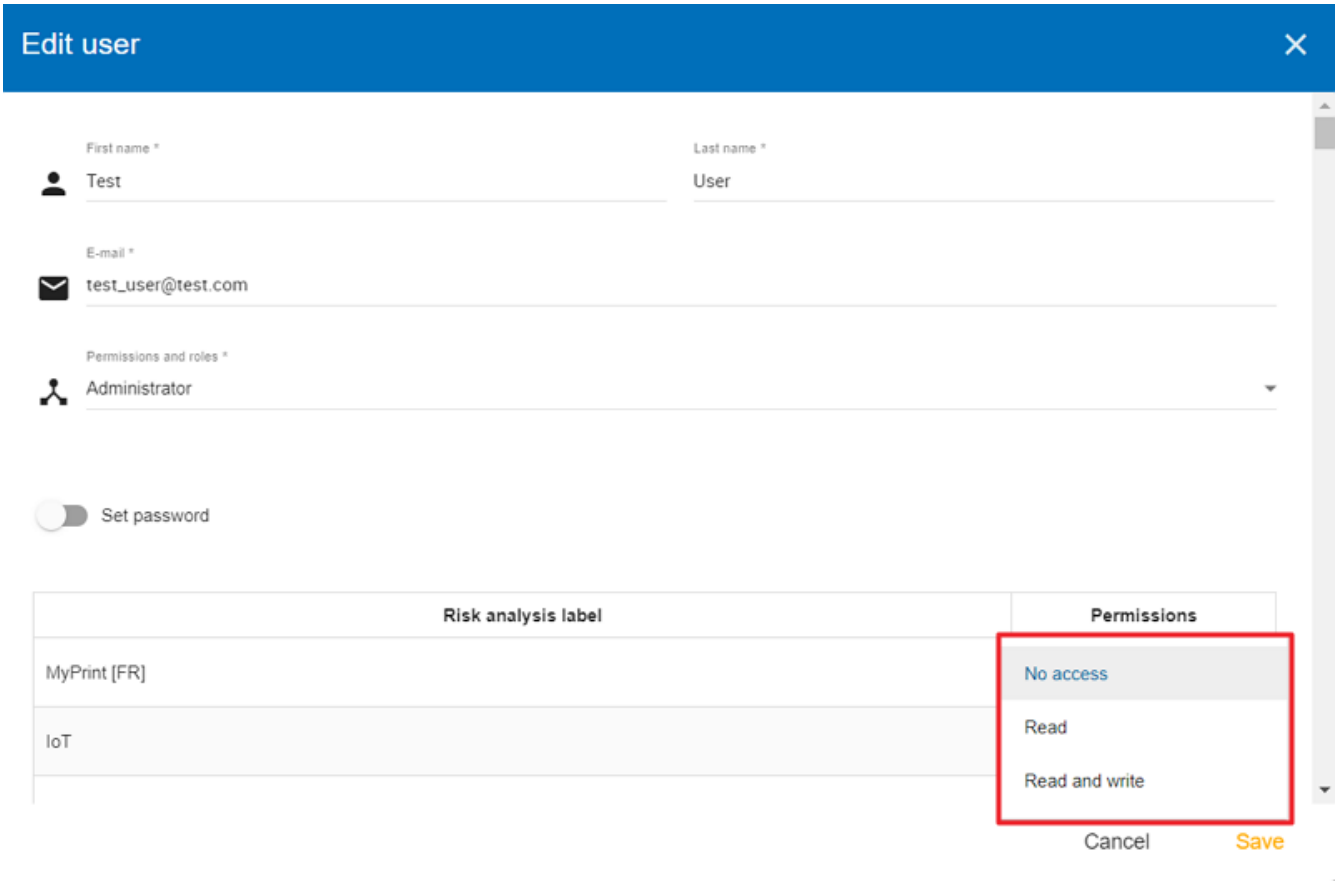
Edit a user

After clicking on the pencil icon , the following screen appears:



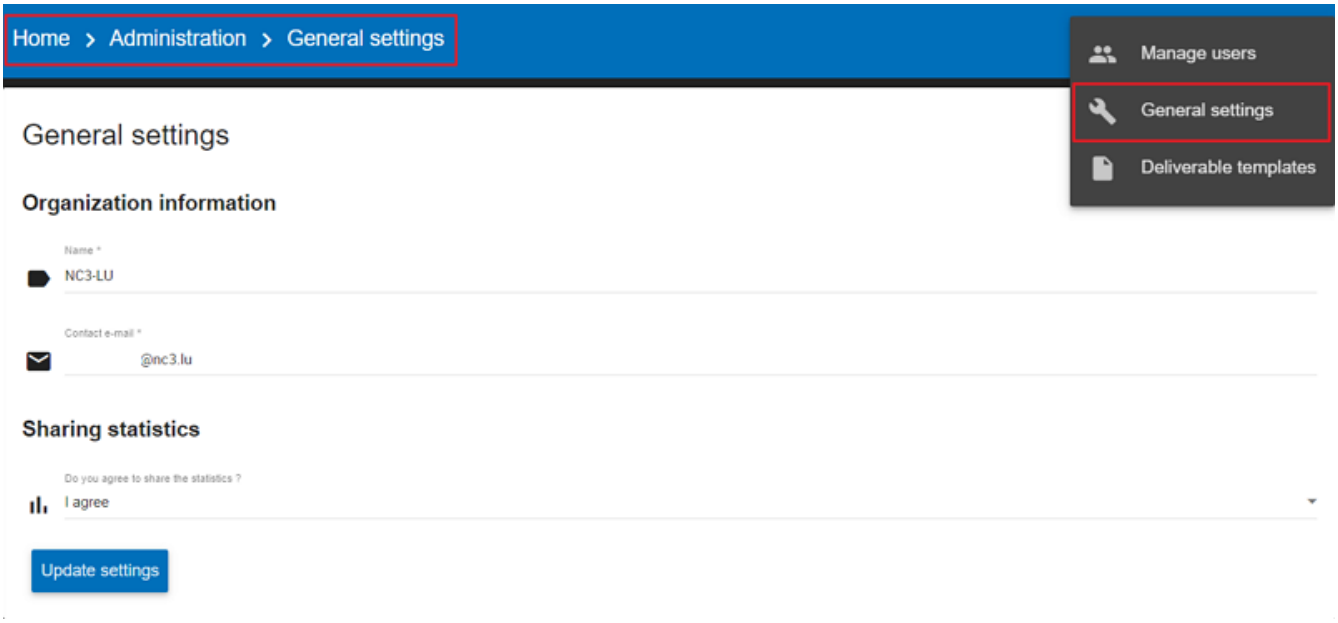
1. General information (First name, Last name, E-mail address).
2. Permissions and roles (`Administrator` or/and `User`, `Global dashboard`).
3. Set password
4. Permissions (No access, Read, Read and write)

Once you click on the down-pointing triangle, the three options for permission levels become visible.



3.1.2. General settings

Click on the gear ison in the top right-hand corner, then select the second menu item from the submenu. The ‘General settins’ window opens with two sections: 'Organization information’ and ‘Sharing statistics’.

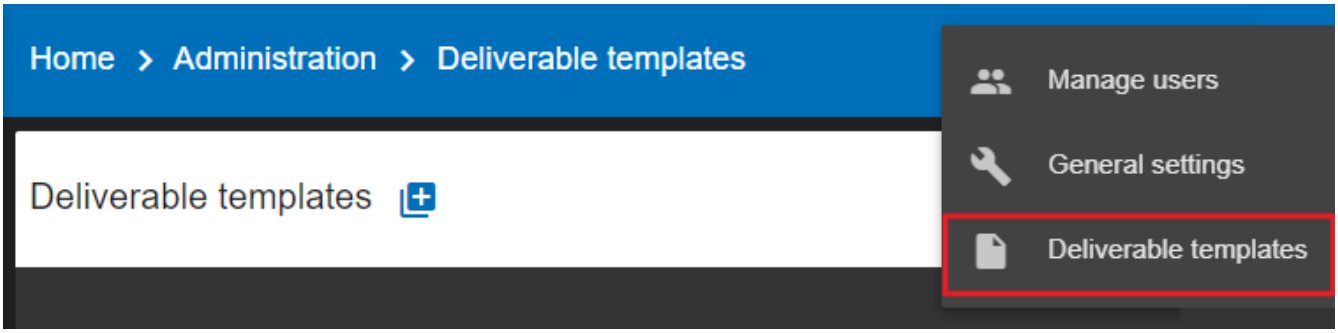


The ‘Organization information’ stores information about the name of your organization and its e-mail address, whereas the ‘Sharing statistics’ section shows whether you agree to share the statistics of your organizations or not. Once you populated the fields for ‘Organization information’ and made your decision regarding ‘Sharing statistics’, click on the ‘Update settings’ button to save your settings.

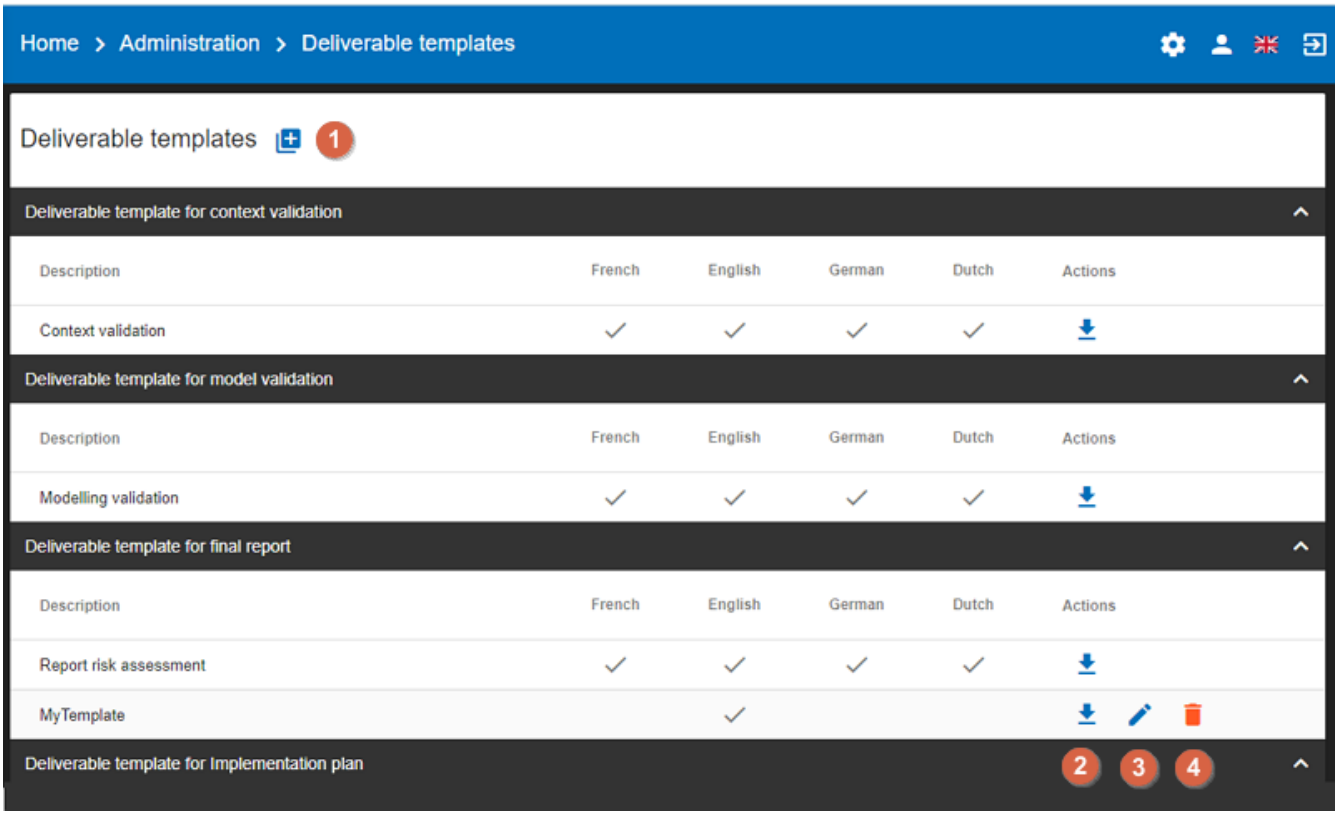
3.1.3. Deliverable templates

In MONARC, you can generate different deliverables (templates) tailored to each organization.

These deliverables are called ‘templates’ within the application. To access the ‘Deliverable templates’ screen, click on the gear icon in the upper right-hand corner and then choose the third submenu called ‘Deliverable templates’.



The ‘Deliverable templates’ screen appears which summarizes all the available templates:



This view summarizes all the available templates. You can perform the following actions on this screen:

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

The default templates are only downloadable, they cannot be modified or deleted.

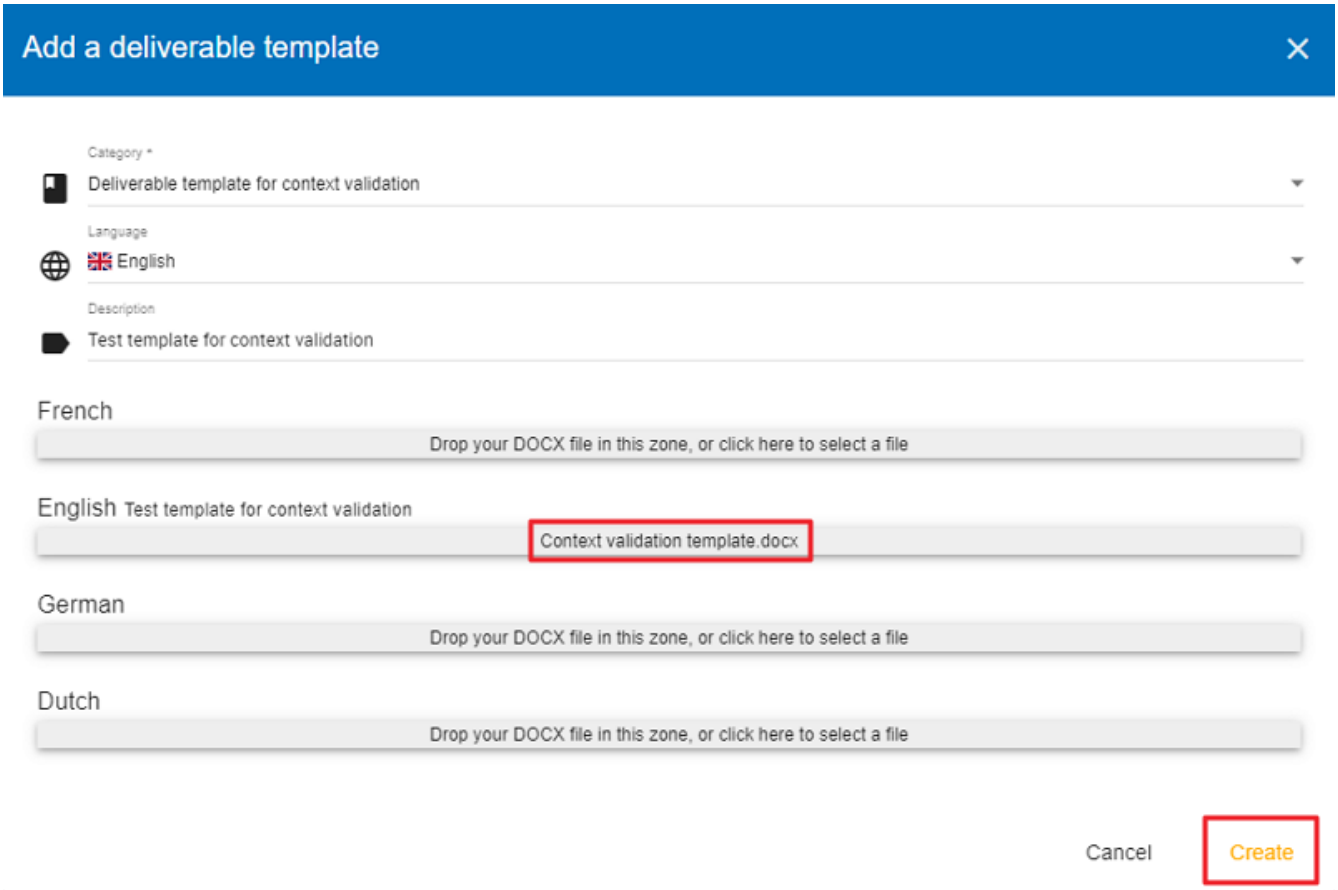
Add a new template

Click on the ‘Add a new template’ button. The following screen appears:

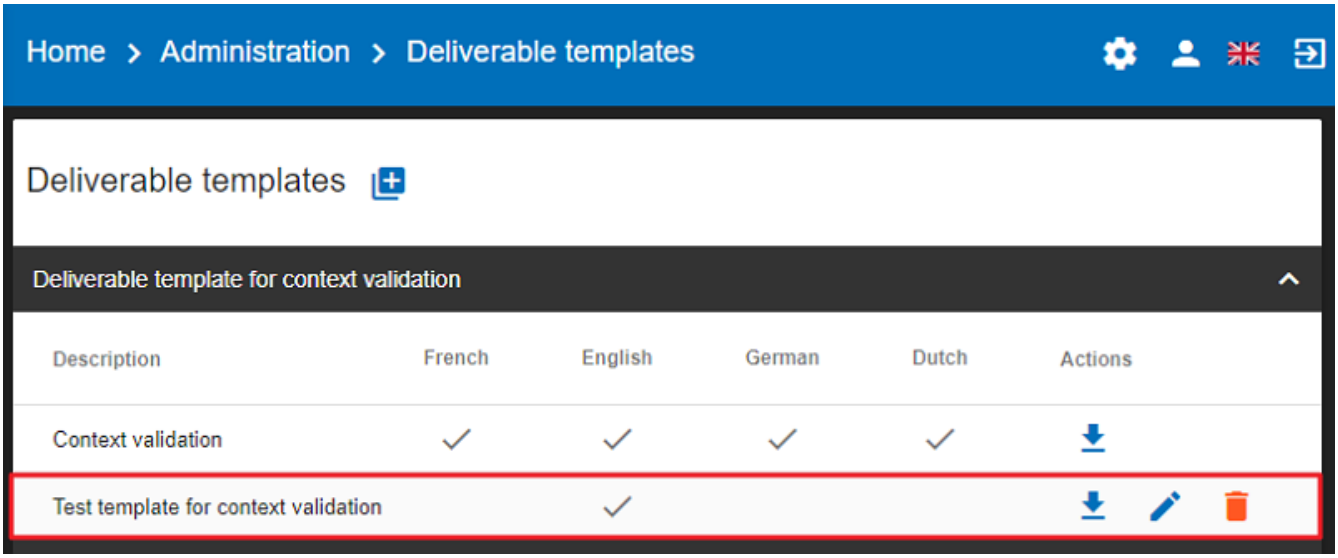
1. Select the `Category` of the template. The category is linked to the different step of the method.
2. Select the `Language` associated with the template.
3. Fill in the `Description` of the new template.
4. Click on the grey area or drag and drop a document on the grey area to `Upload` the template.

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

Once you have finised the above steps, click on the 'Create' button in the lower right-hand corner.



The newly-created template (Test template for context validation) appears on the list within the category (in this case in the Deliverable template for context validation category) you have selected in the deliverable template making process.



List of tags

MONARC allows you to add your delivery template. The template is a document which uses different tags.

> Deliverable templates must be uploaded in Word format (`.docx`). The generated report can be downloaded in Word or PDF format.

Generate a PDF report

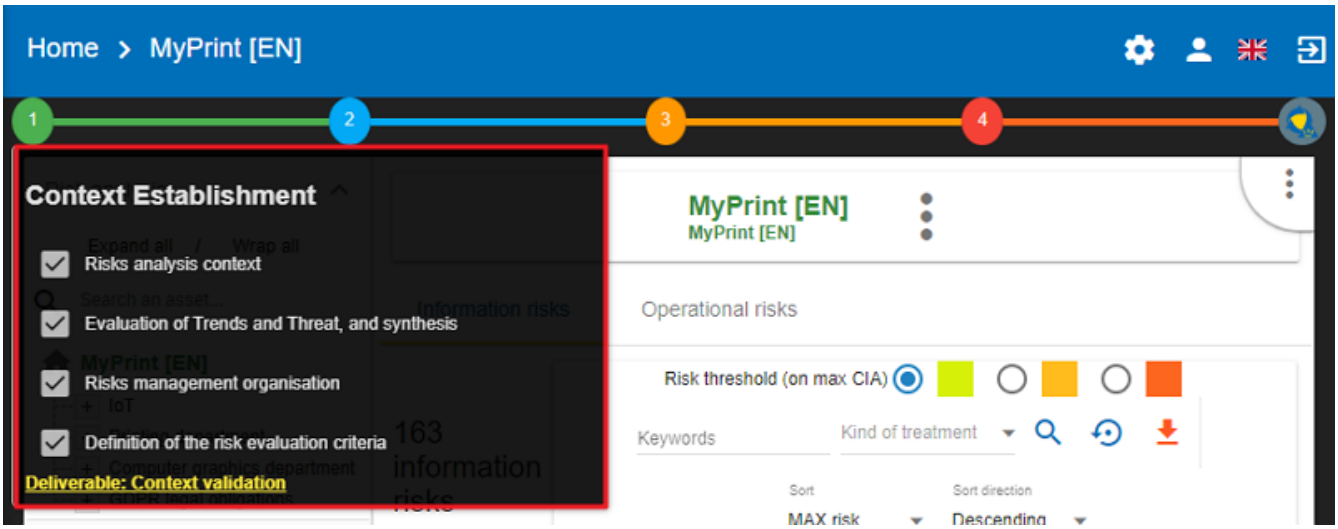
Available from MONARC v2.14.1.

Open the required method step in an analysis and select its `Deliverable` link. Select the template and complete the document metadata as usual. In `Report format`, choose `PDF (.pdf)`, then generate the deliverable. MONARC downloads the generated report as a PDF file. See issue #615 for the associated release item.

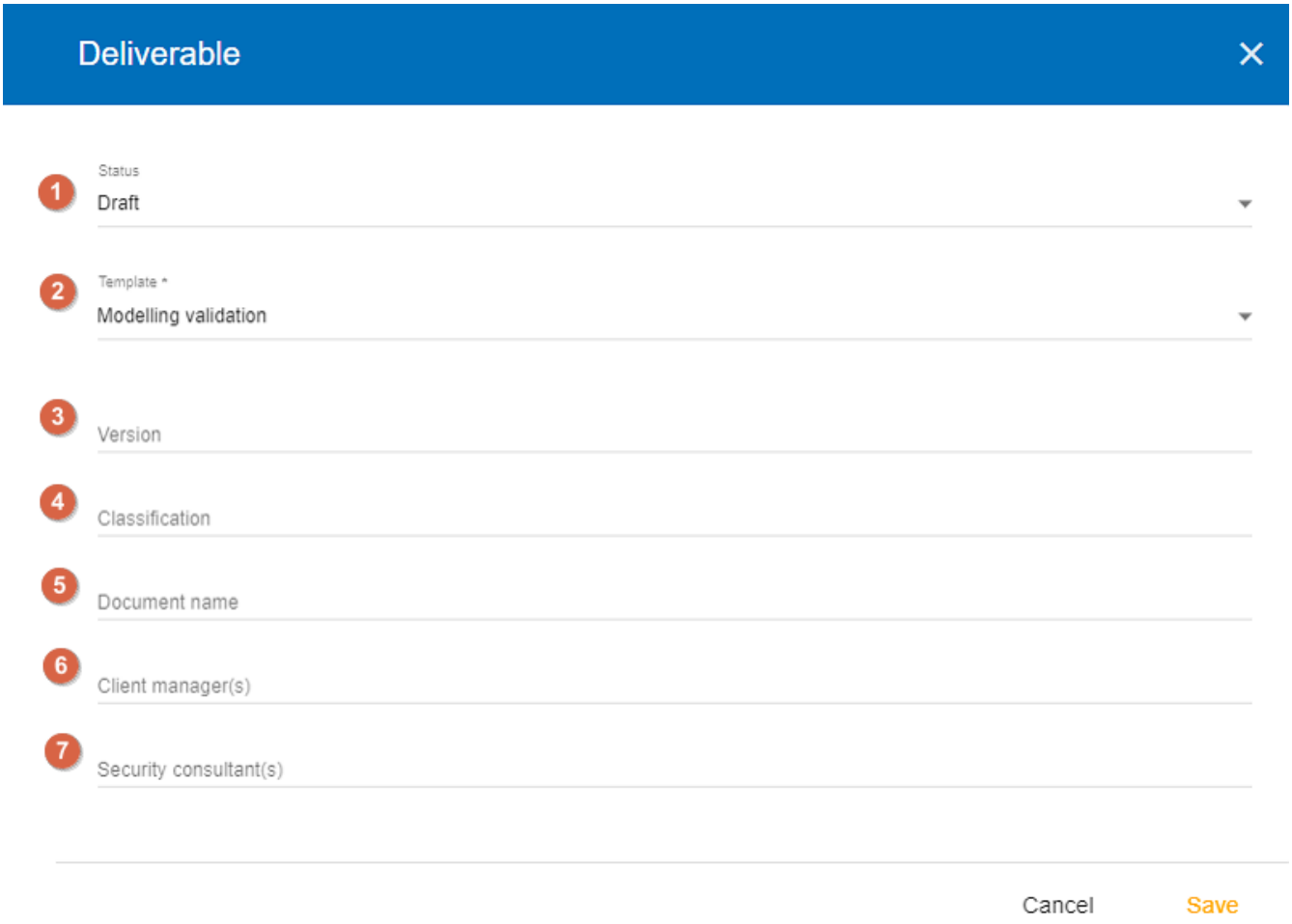
Choose `Word (.docx)` when the report needs further editing. PDF generation uses the same selected template, analysis content, tags, status, version, classification, and document metadata as Word generation.

List of tags for the layout of the document:

All these tags are mainly set in the form depending on the delivery. Open a risk analysis and click on the green icon (1) representing the first step as 'Context Establishment'.



Then, to open the 'Deliverable' window, click on the 'Deliverable: Context validation' link in the lower left-hand corner.

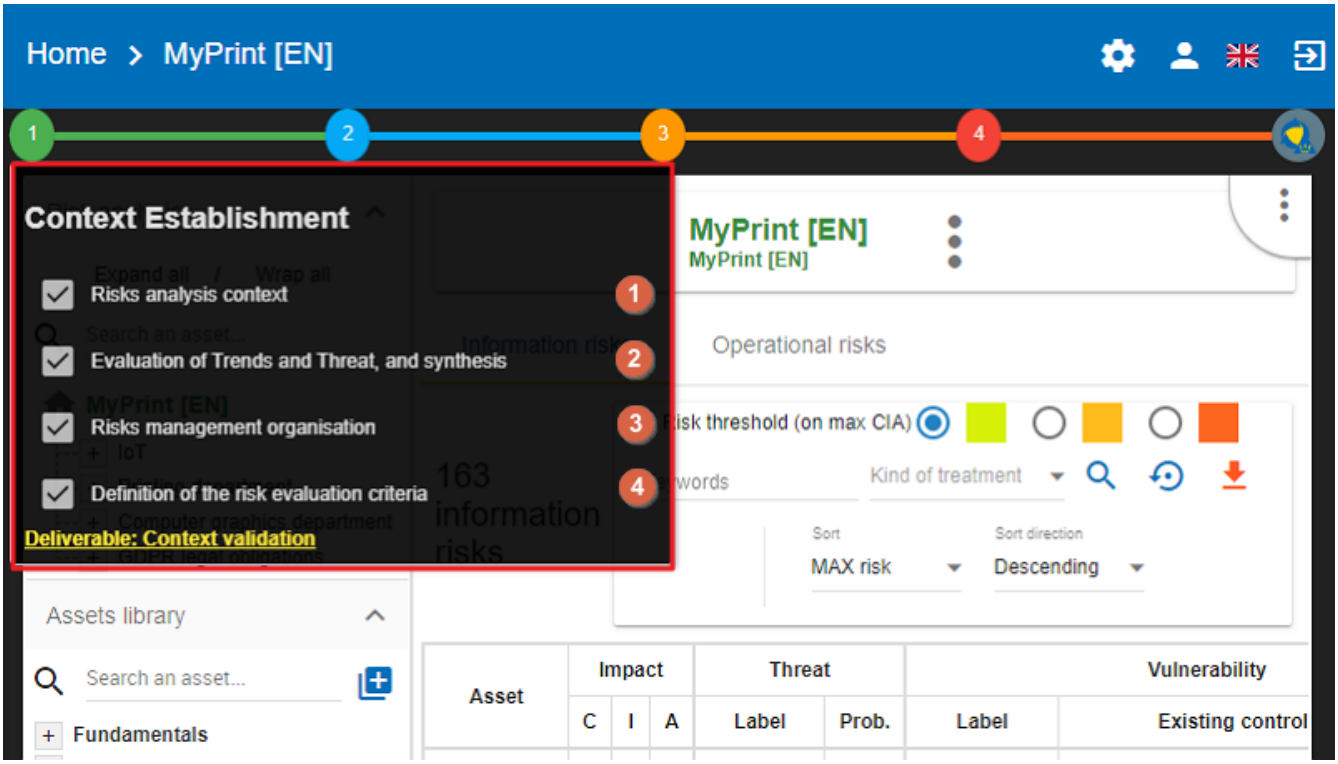


1. `${STATE}`: The status of the document with prefilled value (draft or final).
2. `${TEMPLATE}`:The template you have chosen.
3. `${VERSION}`: The version of the document.
4. `${CLASSIFICATION}`: The classification of the document.
5. `${DOCUMENT NAME}`: The name of the document.
6. `${CLIENT MANAGER(S)}`: The name of the customer(s).
7. `${SECURITY CONSULTANT(S)}`: The name(s) of the security consultant(s) who do(es) the analysis.

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

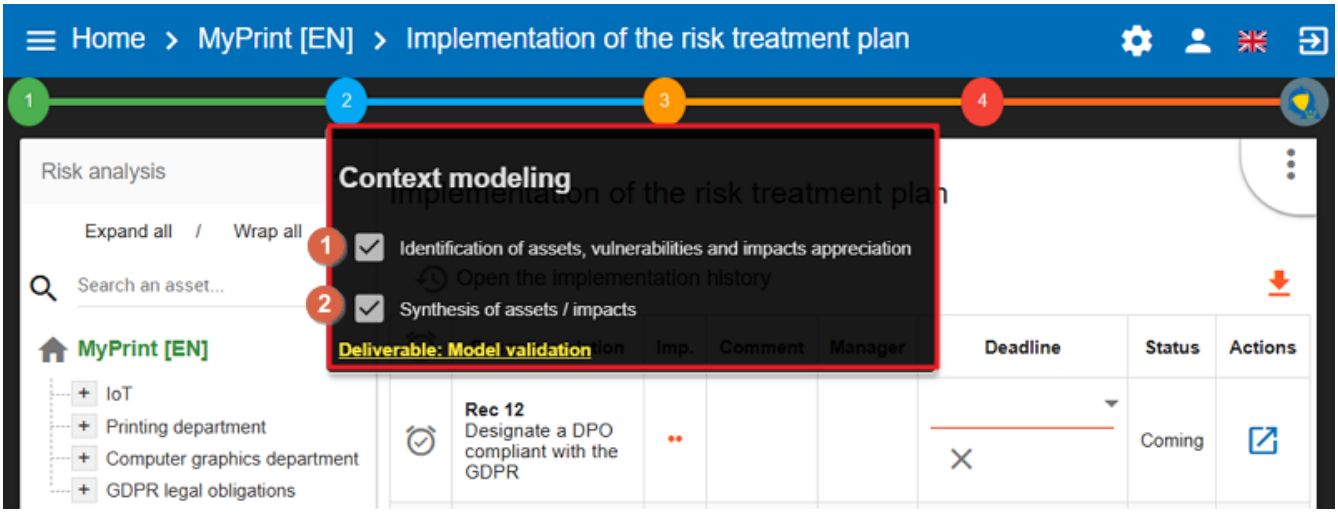
- `${COMPANY}`: Name of the company which comes from MONARC, it's stored in the database and editable in the application.
- `$2023-01-31`: Date of the generation of the document. Field auto-generated by MONARC.

List of the tags from the context establishment:



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. ${TABLE_INTERESTED_PARTIES}: Table of interested parties and their requirements from the `Interested parties & requirements` tab.
5. ${TABLE_REASSESSMENT_TRIGGERS}: Table of the analysis reassessment trigger criteria, including monitoring approach and status.
6. 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.

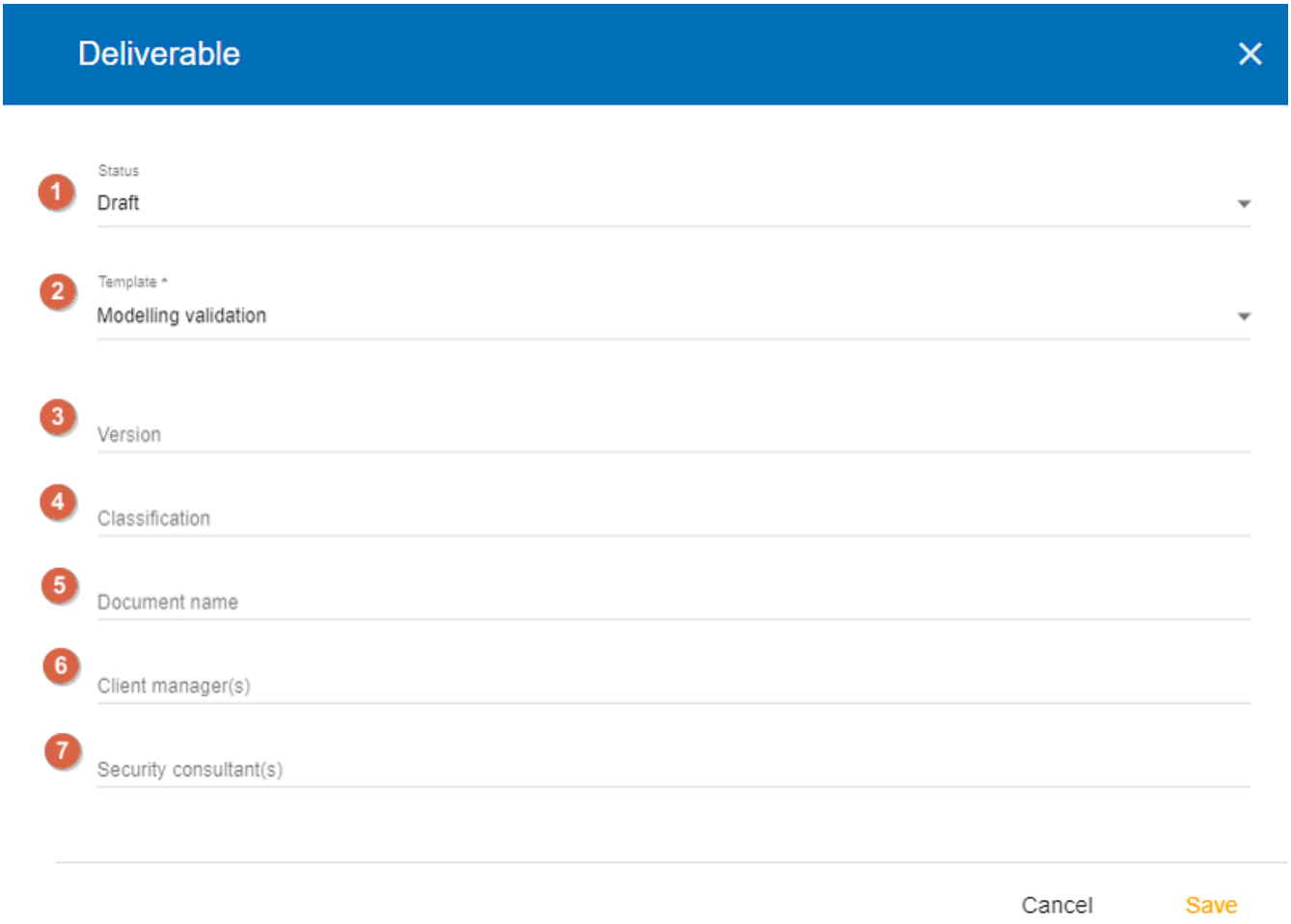
List of tags for the context modeling:



1. Identification of assets, vulnerabilities and impacts appreciation
2. Synthesis of assets/impacts
   - `${SYNTH_ACTIF}`: Free text which comes from the step: “synthesis of assets/impacts”.

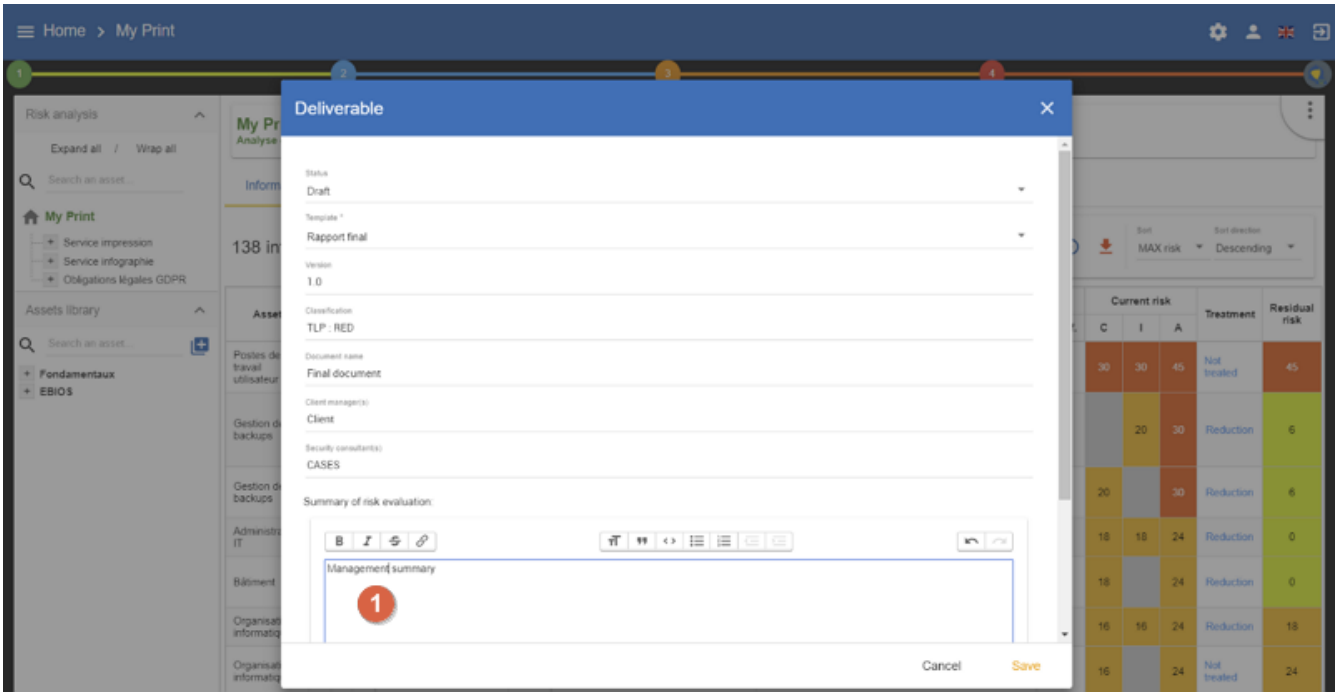
- `${IMPACTS_APPRECIATION}`: A table which is generated by MONARC. It represents the impacts/consequences of the top-level assets.

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



1. Status: The status can be ‘Draft’ or ‘Final’

2. Template: From the dropdown menu, please choose a template you want to use
3. Version:
4. Classification:
5. Document name:
6. Client manager(s)
7. Security consultant(s)



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_RISK_OWNERS}: A table of supervisors, their roles, linked users, and assigned 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.

User account

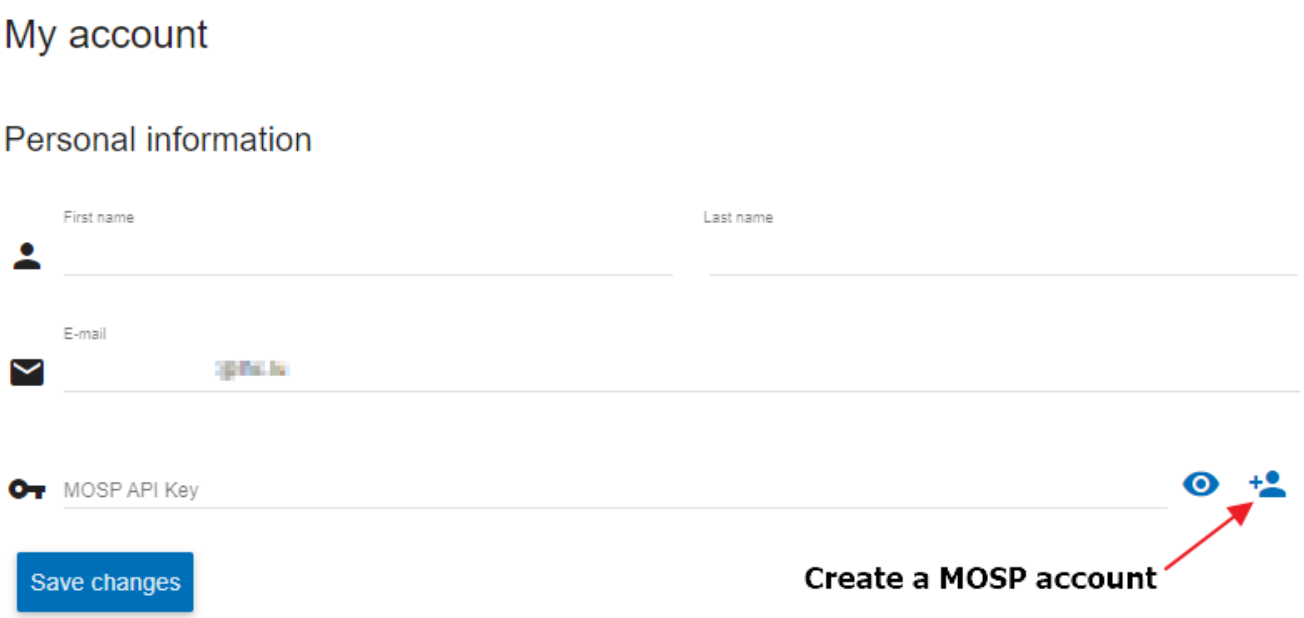
To get to the 'My account' page, click on the second icon in the top right-hand corner of the application:

The 'My account' page appears which has three sections

- Personal information
- Security
- Danger zone

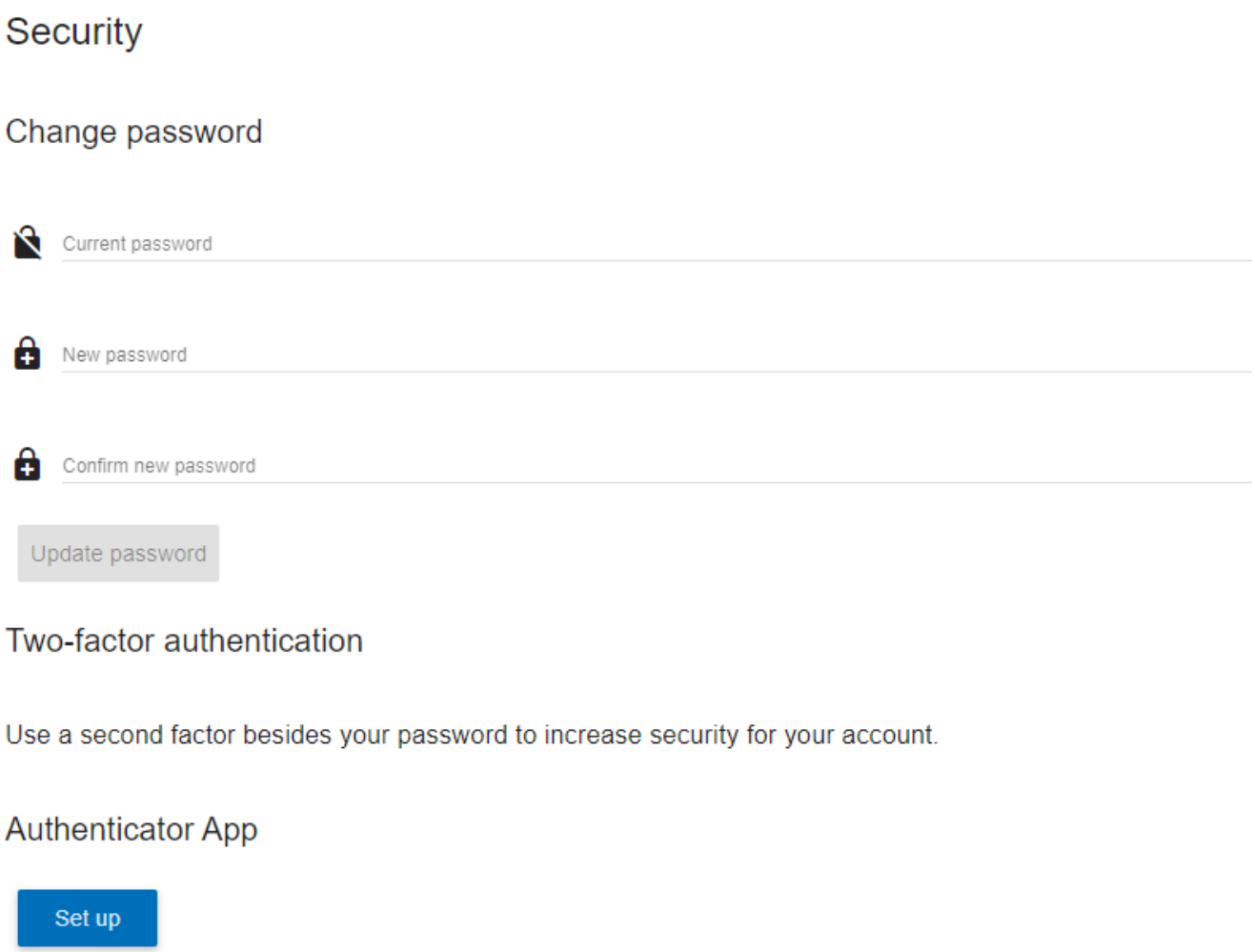
Personal information

The Personal information section stores the first name, the last name and the email address of the user. You can also create a MOSP account by clicking on the person plus icon in the far right as indicated in the below screenshot:

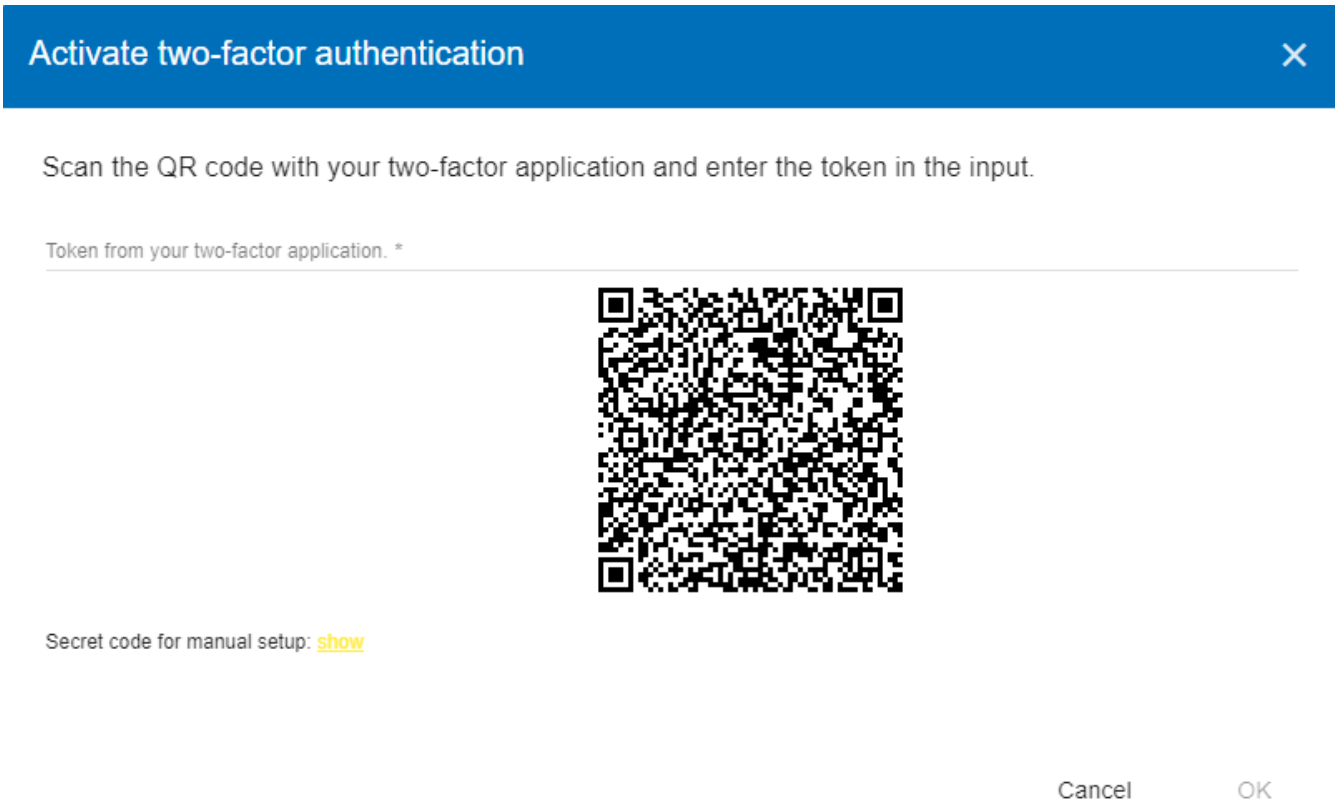


Security

In the security section, you can create a new password and set up two-factor authentication. Once you typed in your new password, click on the 'Update password' button.



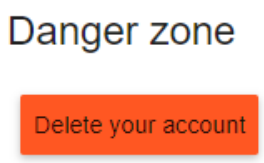
Click on the ‘Set up’ button at the bottom of this section to set up your two-factor authentication. If you click on the ‘Set up’ button, the ‘Activate two-factor authentication’ screen appears:



Please scan the QR code with your phone and follow the steps to set up 2FA.

Danger zone

The third section is called the 'Danger zone'. This is where you can delete your account.



Interface language

To change the 'Interface language', click on the third icon in the top right-hand corner of the application and choose your preferred language from the dropdown menu.

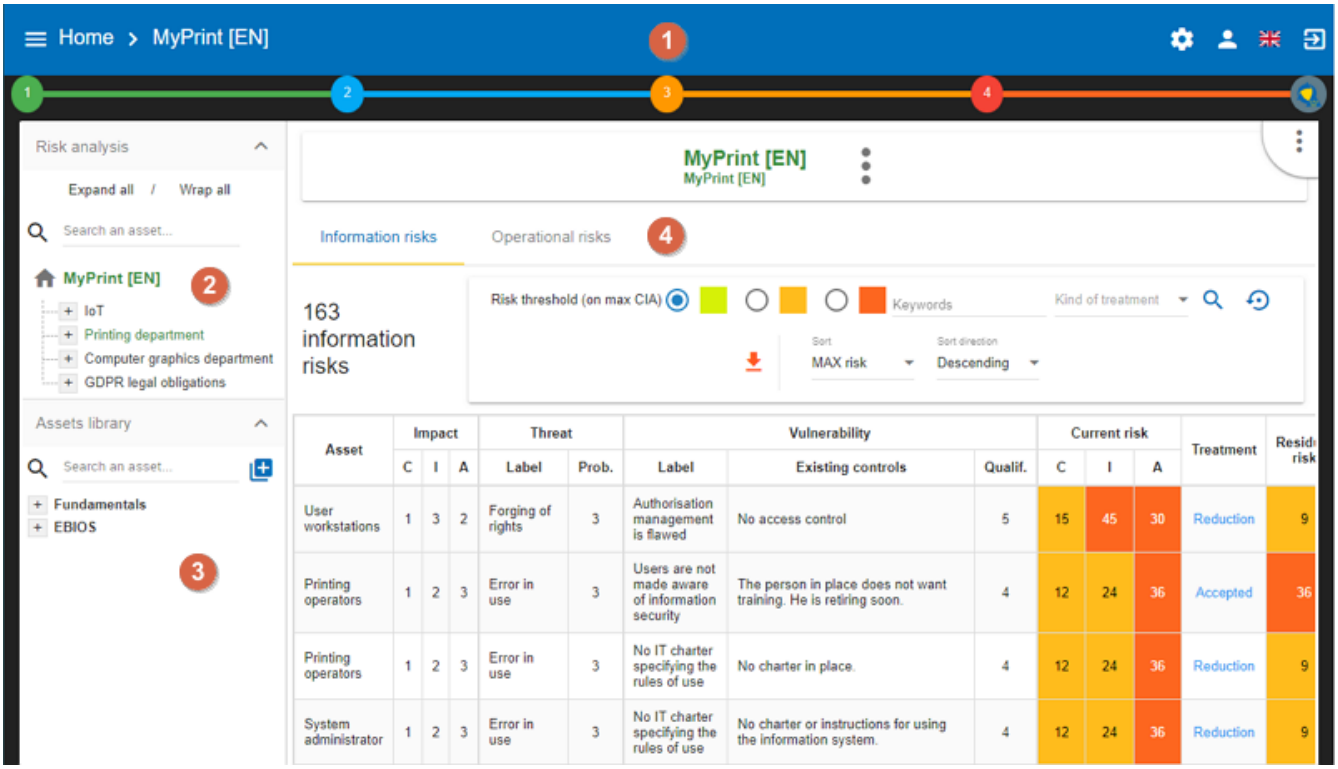
There are five interface languages in the system as follows:

- French
- English
- German
- Dutch
- Spanish

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

Chapter 4. Analysis Management

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

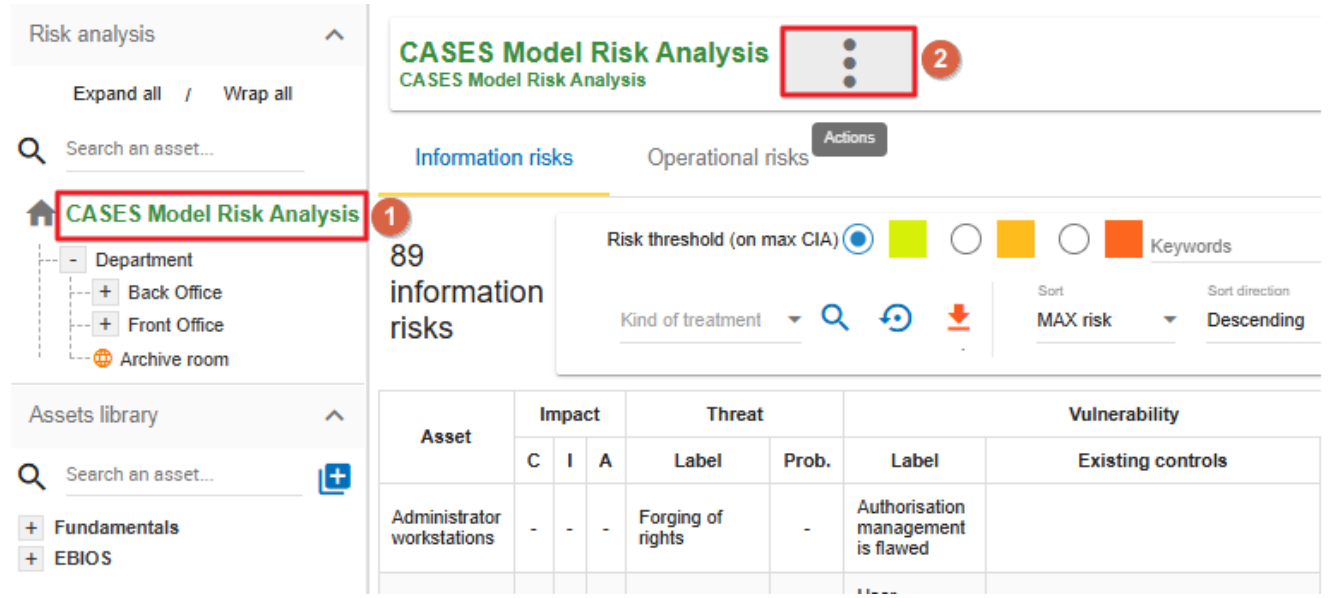


1. Access to the steps of the method: Click on the numbers from 1 to 4 to access the menus which follow the step-by-step method (see Method steps call).
2. Risk Analysis area: allows you to structure the assets of the analysis hierarchically by using the *Drag and Drop* function (hold down the left mouse button to move an asset). (See Information Risks and Operational Risks)
3. Asset library area: Asset storage. The *drag-and-drop* function must be used to place these assets in the analysis (to move them to the Risk Analysis Area) (see Library).
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.

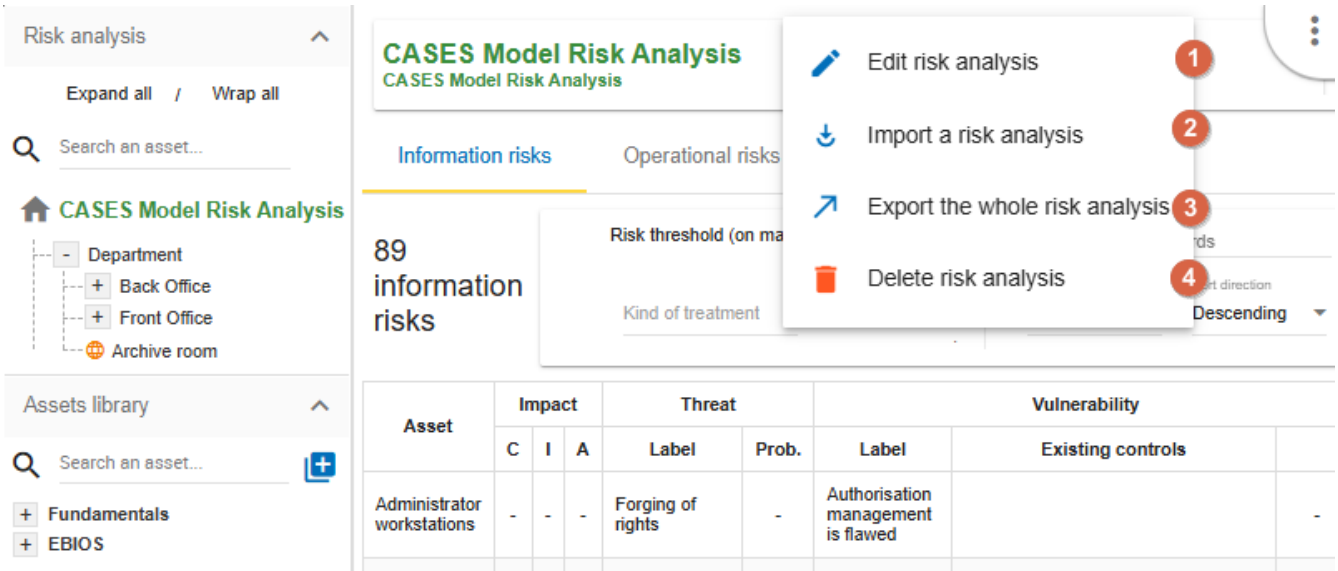
4.1. Risk analysis management

You can manage your analysis in two steps as follows:

1. First, click on the name of the analysis
2. Second, click on the three-dot context menu (if you hover your mouse over the menu, a tooltip 'Actions' appears)



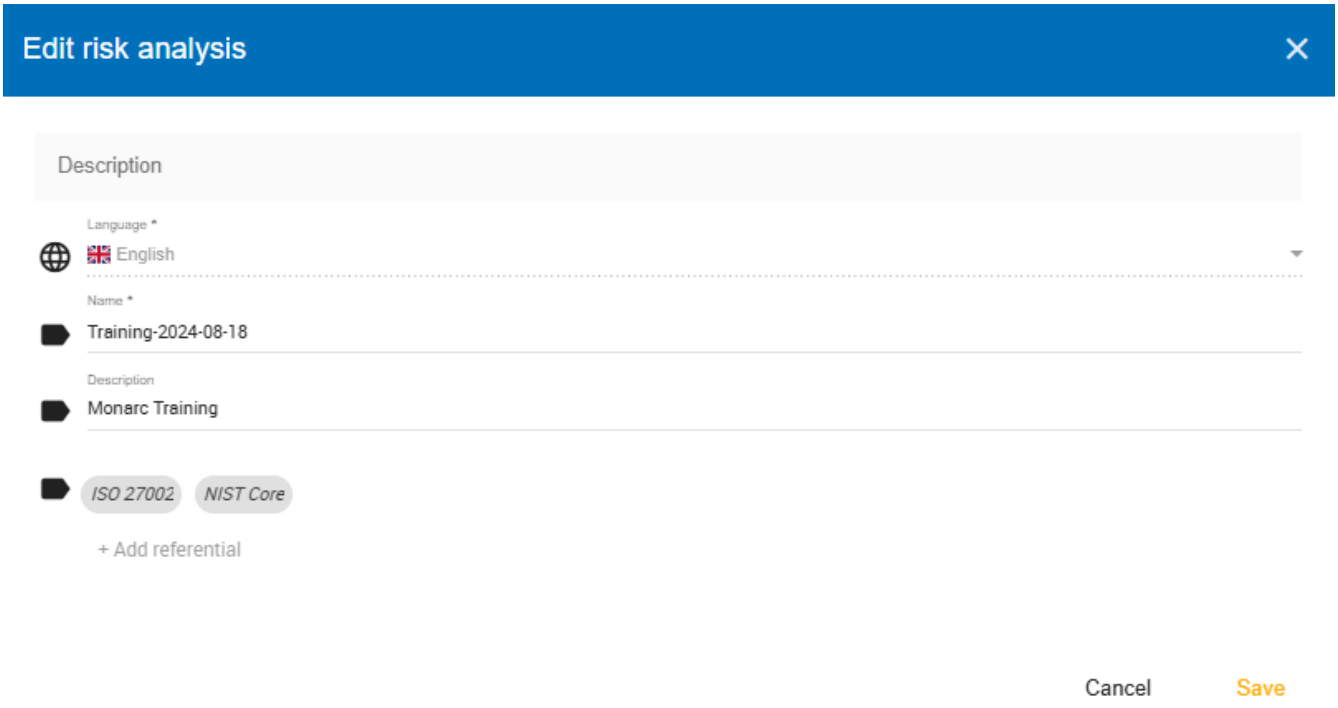
When you click the three-dot context menu, the following options appear:



ISO 27005:2022 adaptation

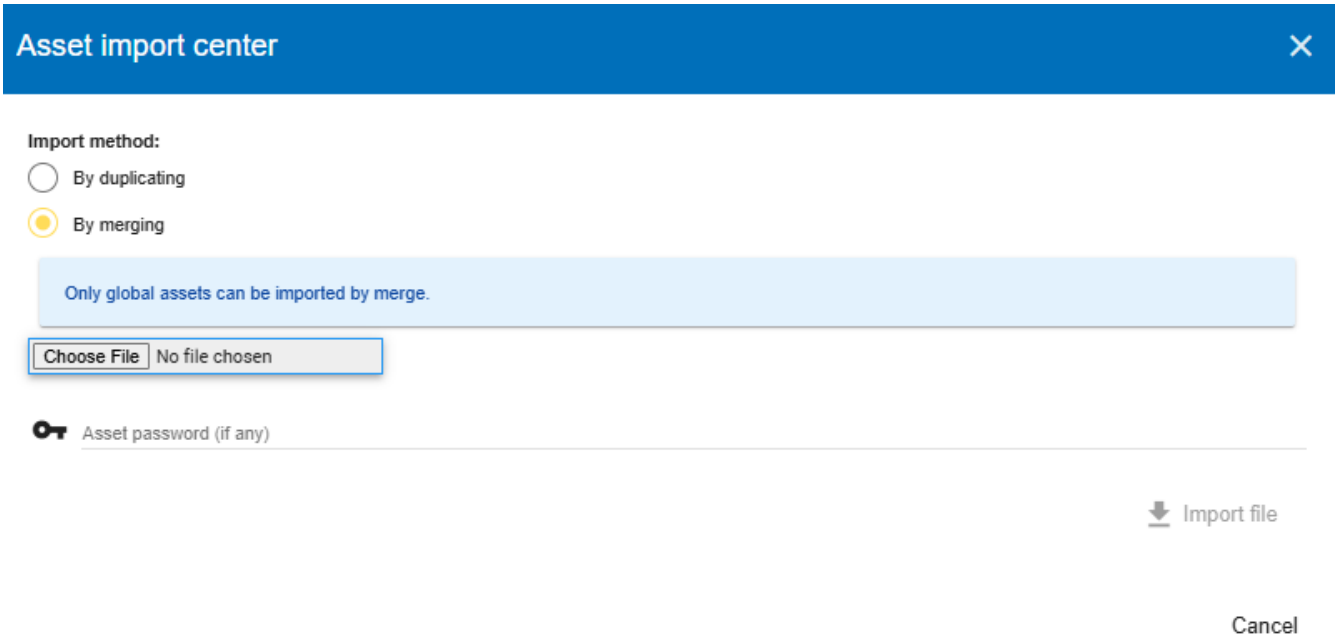
The analysis actions menu now also gives direct access to `Reassessment trigger criteria` and `Supervisors`. These two dialogs are analysis-level management screens used to maintain review triggers, monitoring approaches, supervisor roles, linked users, and approval responsibilities.

1. Edit risk analysis - use this option in case you want to modify your existing risk analysis. This option allows you to modify the name, the description of the analysis, and add or remove linked referential. The Edit risk analysis pop-up appears:



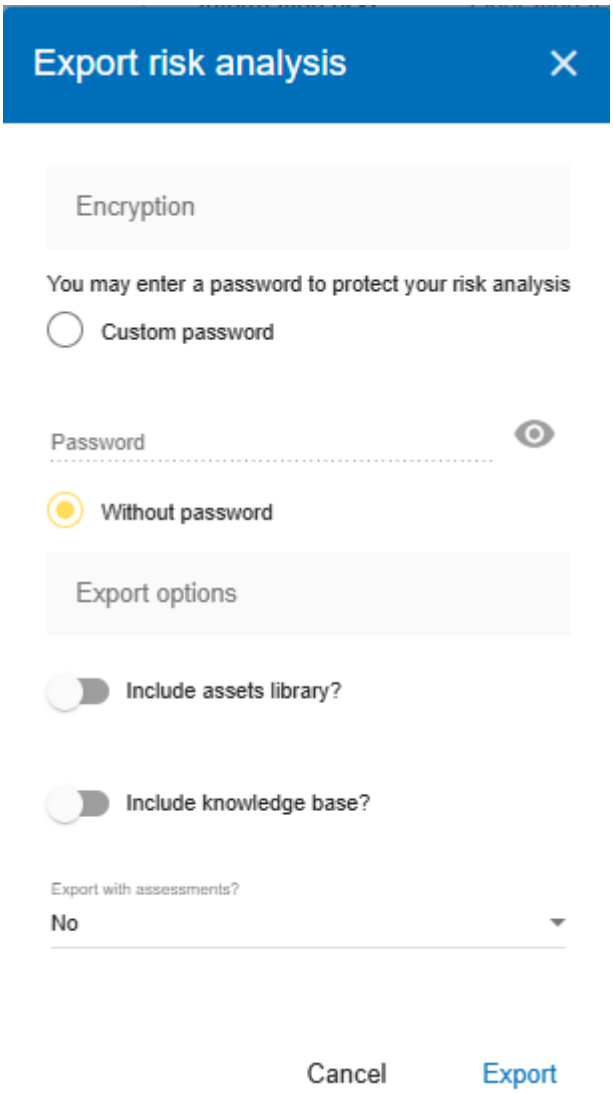
2. Import a risk analysis - you can import a complete risk analysis. The file format is JSON and the structure can be viewed by exporting an analysis. There are 2 possible options of the export:
   - By merging (default). When matched assets names are not duplicated in the library.
   - By duplication. When the library assets are duplicated in case if presented before. The analysis assets will also be duplicated.

> An analysis can be only imported when the language of its creation is the same as the current analysis (into which import is performed)!



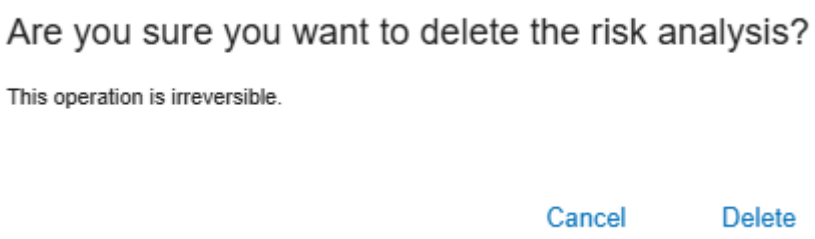
3. Export the whole risk analysis - you can export the whole analysis with or without the assets library and the knowledge base. The export of the analysis can be done with the following options:

- The export file can be protected by a password if it is set (Custom password option).
- "Include assets library?" The whole assets library is included in the export if the option is selected.
- "Include knowledge base?" The whole knowledge base is included in the export if the option is selected.
- “Export with assessments?” All the evaluations are included. Optionally can be added or not different analysis evaluation criteria (Options section).



4. Delete risk analysis

If you click on the link 'Delete risk analysis', the following pop-up appears:



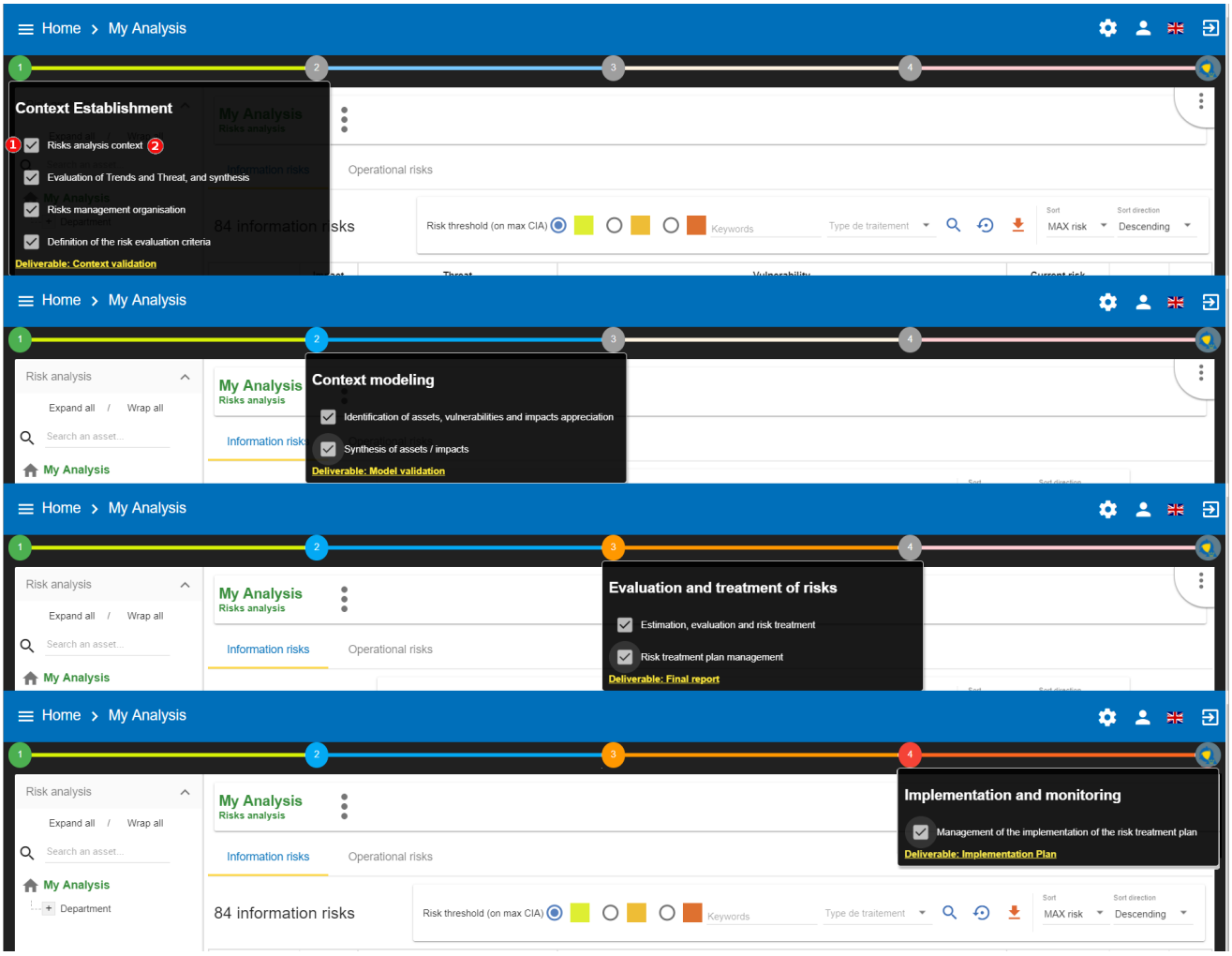
Please note that the operation is irreversible.

ISO 27005:2022 adaptation

When exporting a risk analysis with assessments, the export options now also include switches for `Interested parties & requirements` and `Reassessment trigger criteria`. Supervisor data is exported with the analysis structure so risk-owner and approval assignments can be preserved on import.

4.2. Method steps call

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

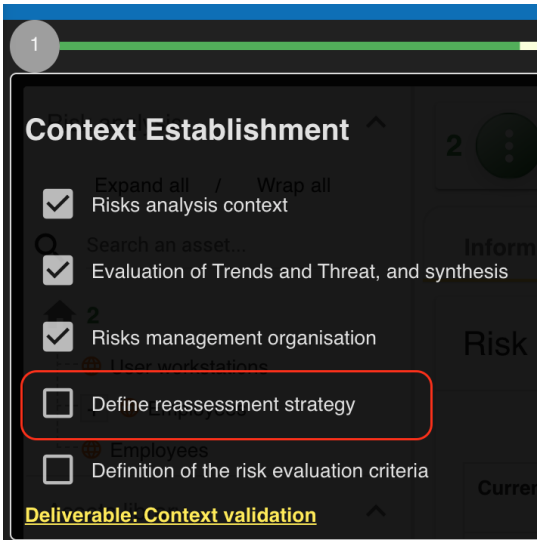


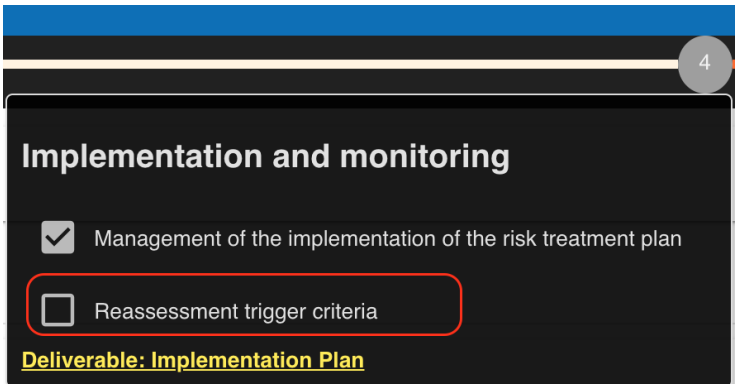
1. Ticking boxes change the progress of the method.
2. Click on the label, and call the contextual management sub-screen.

More information about method steps. Consult the **Method Guide**.

ISO 27005:2022 adaptation

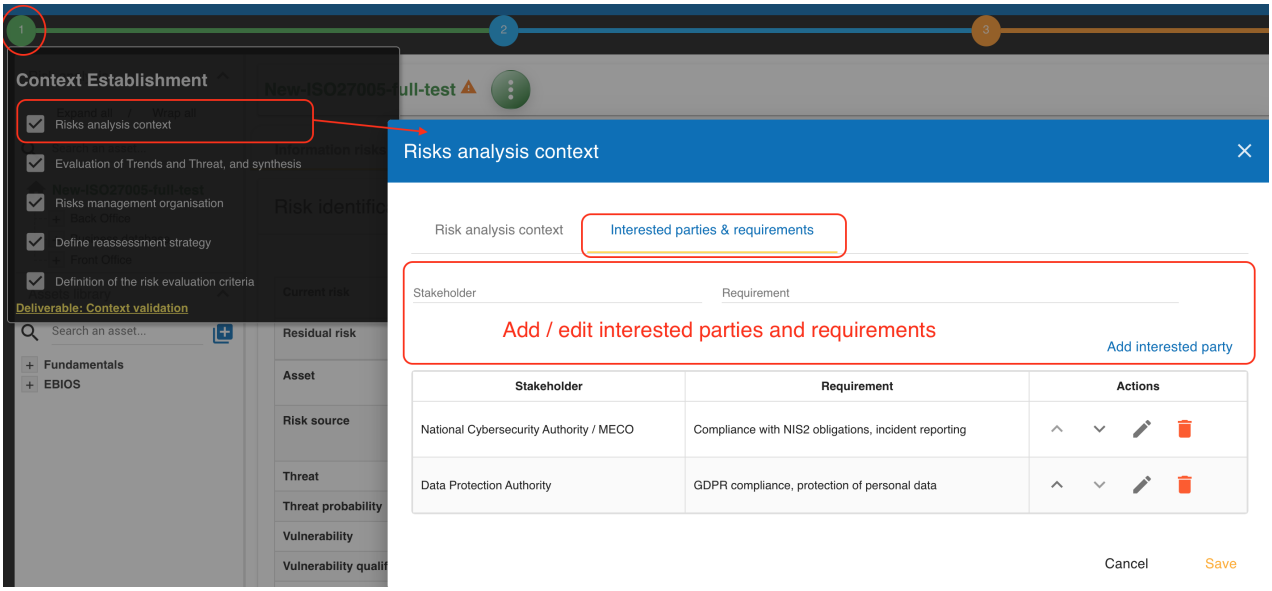
`Reassessment trigger criteria` can be opened from two method substeps: `Define reassessment strategy` in step 1, `Context Establishment`, and `Reassessment trigger criteria` in step 4, `Implementation and monitoring`.





ISO 27005:2022 adaptation

In the `Risk analysis context` sub-screen of step 1, MONARC now provides an additional tab named `Interested parties & requirements`. This tab is used to maintain stakeholders and their requirements alongside the existing free-text context description.

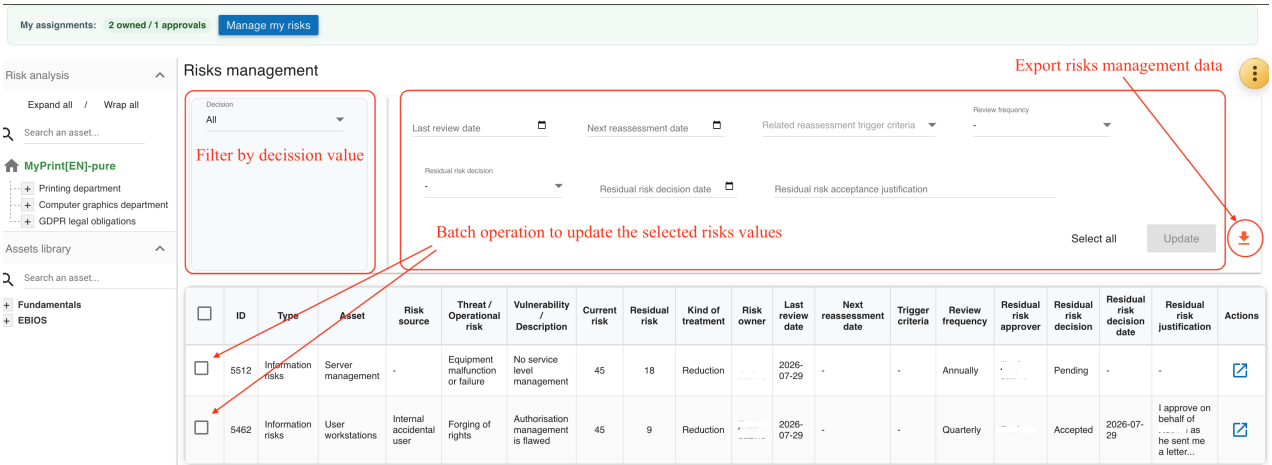


4.3. Risks management

ISO 27005:2022 adaptation

If the current user is linked to an active supervisor in the analysis and has assigned risks, the tools menu exposes a dedicated `Risks management` view. The analysis header also displays a `My assignments` panel with owned and approval counts plus a direct `Manage my risks` action.

The `Risks management` view only lists the risks in which the linked supervisor is involved. It supports role-based batch updates for review metadata and residual-acceptance decision fields.



Select one or more information or operational risks, enter only the values that should change, then select `Update`. The table keeps the following fields visible so the user can assess the selected register before acting: `Risk owner`, `Risk source`, `Last review date`, `Next reassessment date`, `Related reassessment trigger criteria`, `Review frequency`, `Residual risk approver`, and residual-acceptance details.

The available batch fields depend on the linked supervisor role:

- A `Risk owner` can update `Last review date`, `Next reassessment date`, related trigger criteria, and

`Review frequency` for risks they own.

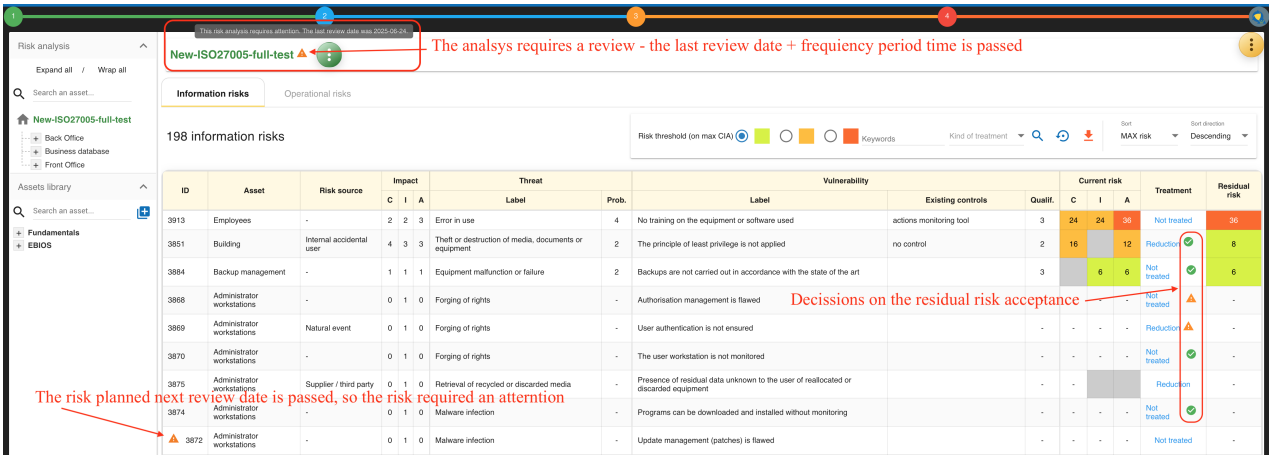
- A `Residual risk approver` can update the residual-risk decision, decision date, and justification for risks they are allowed to approve.
- A supervisor with both roles receives both groups of fields.

Risk owner, risk source, and residual-risk approver are display-only in this view. Open the risk sheet to change their assignments. After an update, MONARC displays the number of updated and skipped risks. Any skipped row is listed with its reason.

The download button exports the currently displayed risks-management list as a CSV file. The export includes the table fields above, including risk source, owner, reassessment schedule, linked trigger criteria, review frequency, approver, and residual-risk decision data.

ISO 27005:2022 adaptation

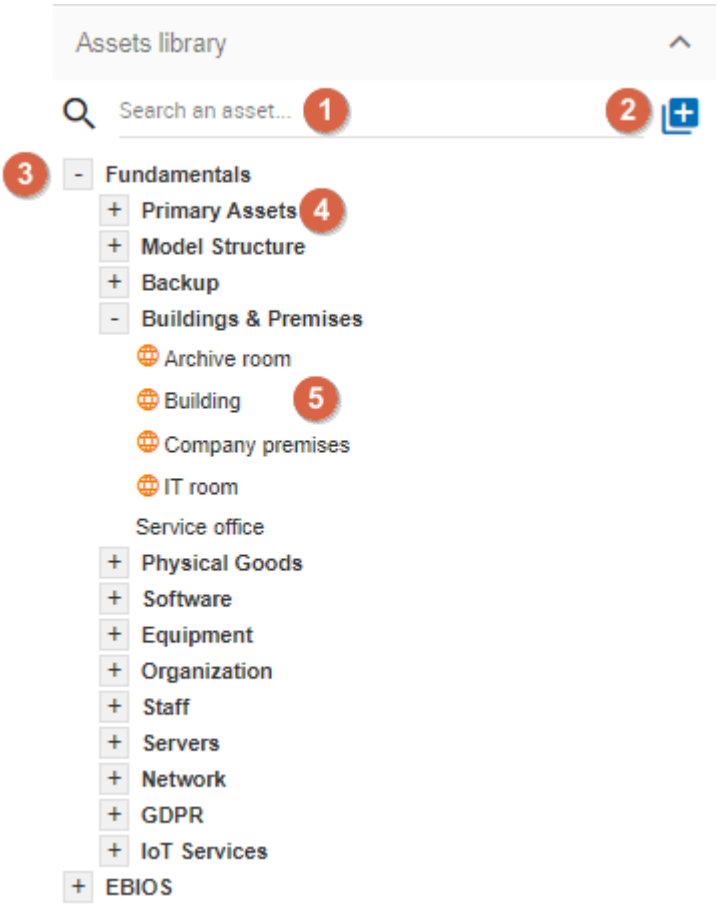
Risks with an overdue next reassessment date display the same orange warning icon in this view as in the ordinary information- and operational-risk tables. A green check-circle next to a treatment shows an `Accepted` residual-risk decision; an orange warning icon shows `Not accepted`. Hover an icon to see its explanation.



4.4. Library

4.4.1. Organization of assets

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



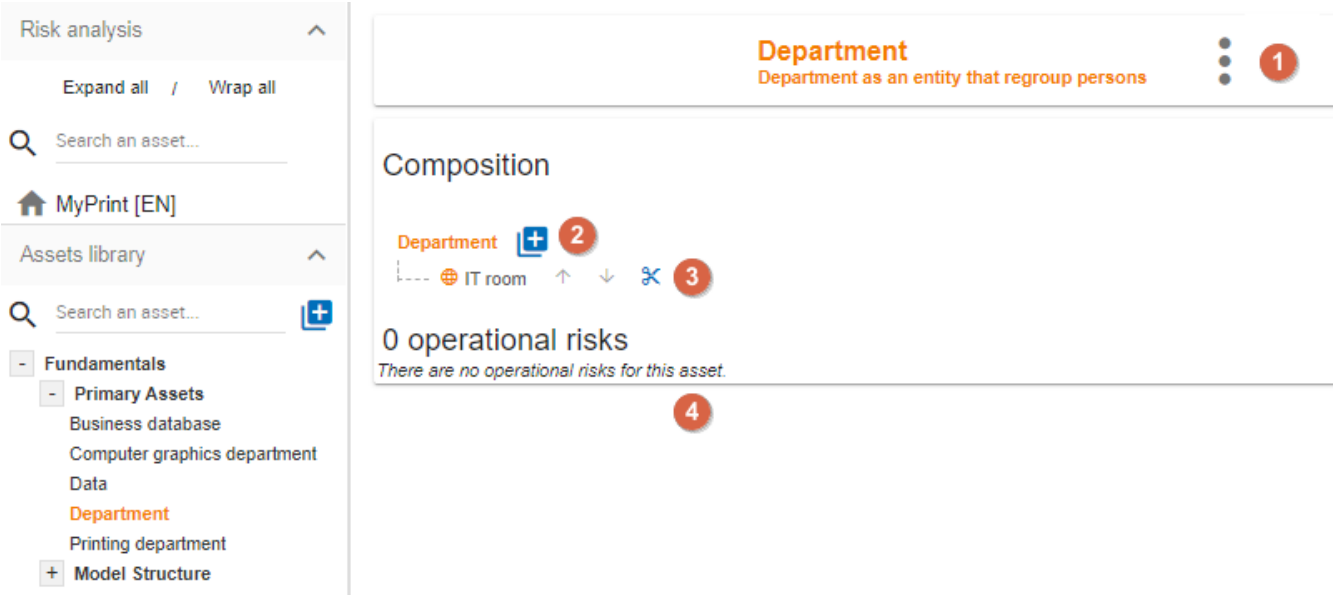
1. Search area in order to quickly find an asset.
2. Button for creating/importing assets (see Create an Asset).
3. Categories level of the Library. There are usually two categories as follows:
   1. `Fundamentals`: Contains all default assets offered by NC3.
   2. `EBIOS`: Contains assets inspired by EBIOS. These are assets containing non-optimized risk models.
4. Sub-categories level.
5. Asset level: These are the assets that must be dragged and dropped to the Risk Analysis area.

4.4.2. Asset Management

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

Primary asset

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



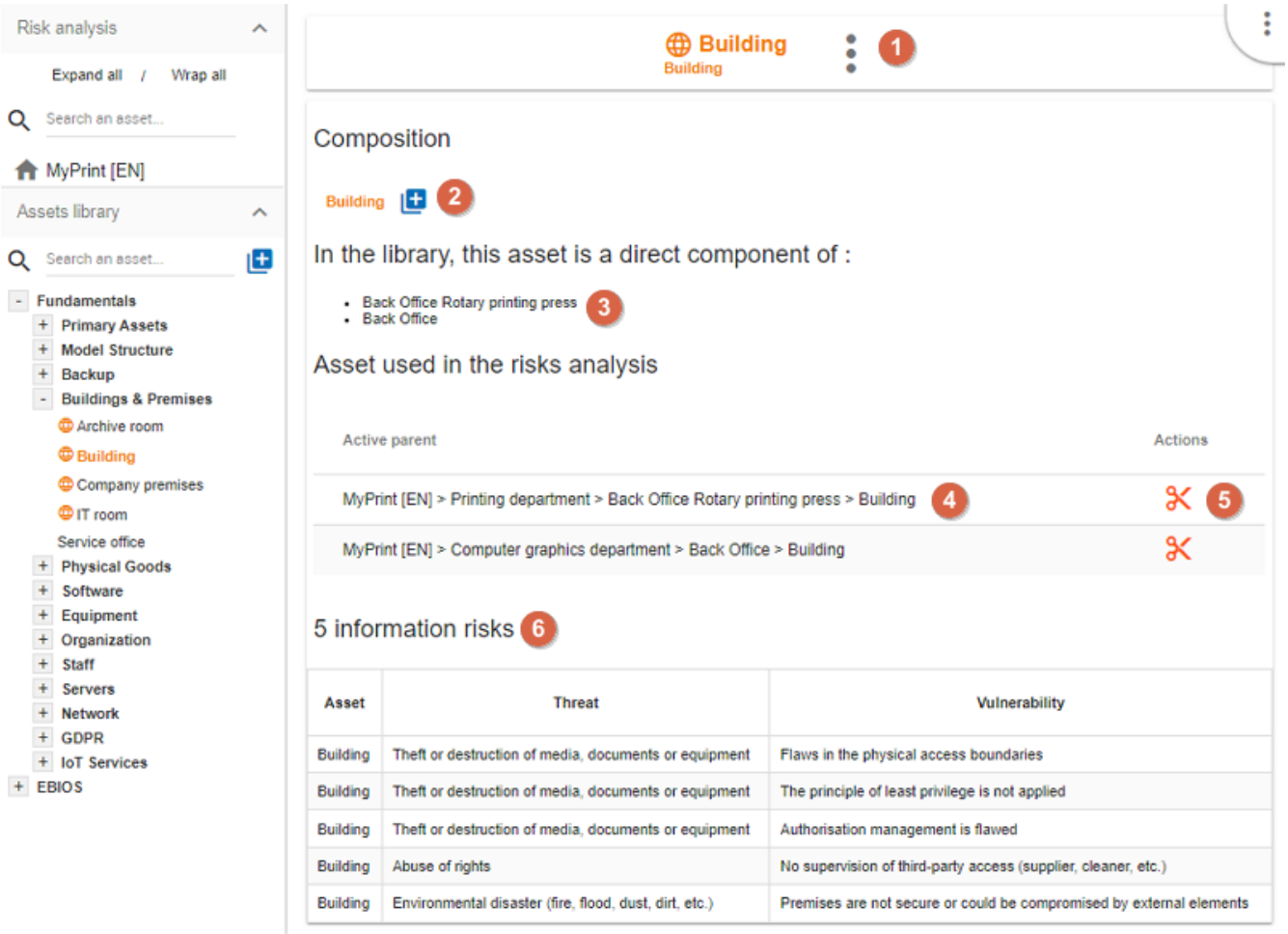
1. Asset management context menu (details in the [Context menu of Library]).
2. Add an existing asset in the structure, creating a composed asset. There is no limit to the asset tree.
3. Ability to detach assets from analysis.
4. Table of operational risks possibly associated with the asset.

Detaching 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`.



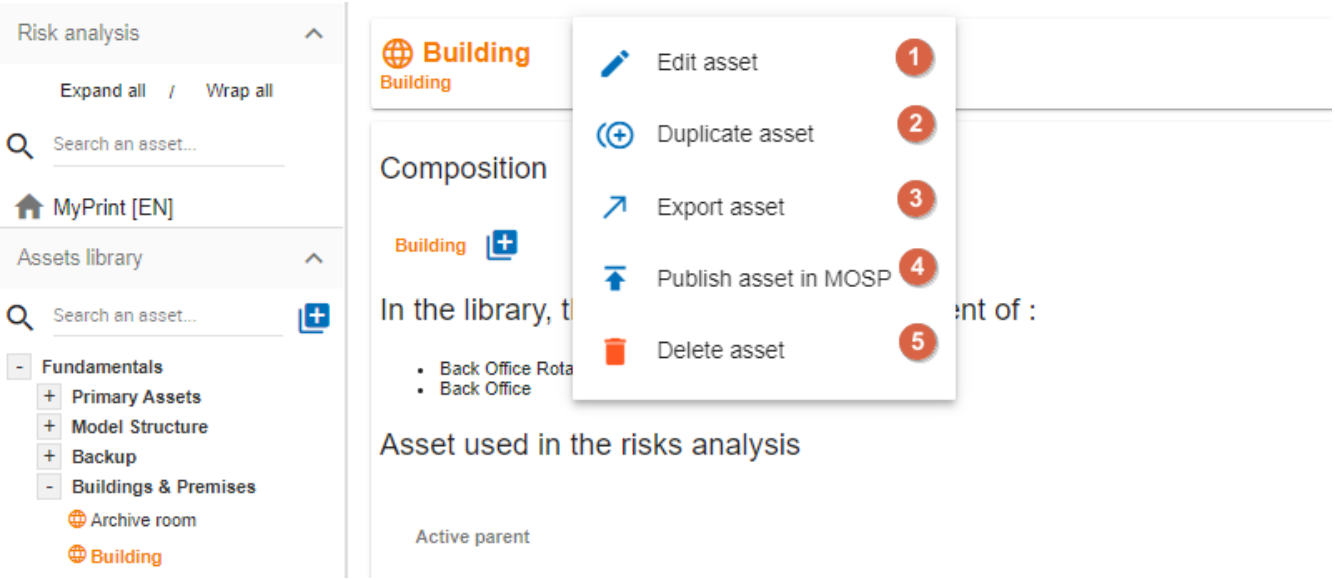
1. Asset management context menu (details in the [Context menu of Library]).
2. Add an existing asset in the structure, creating a compound asset. There is no limit to the asset tree.
3. Indication if the asset is already part of the composition of another asset. In this case, it is already a sub-element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

Detaching 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 the Library

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

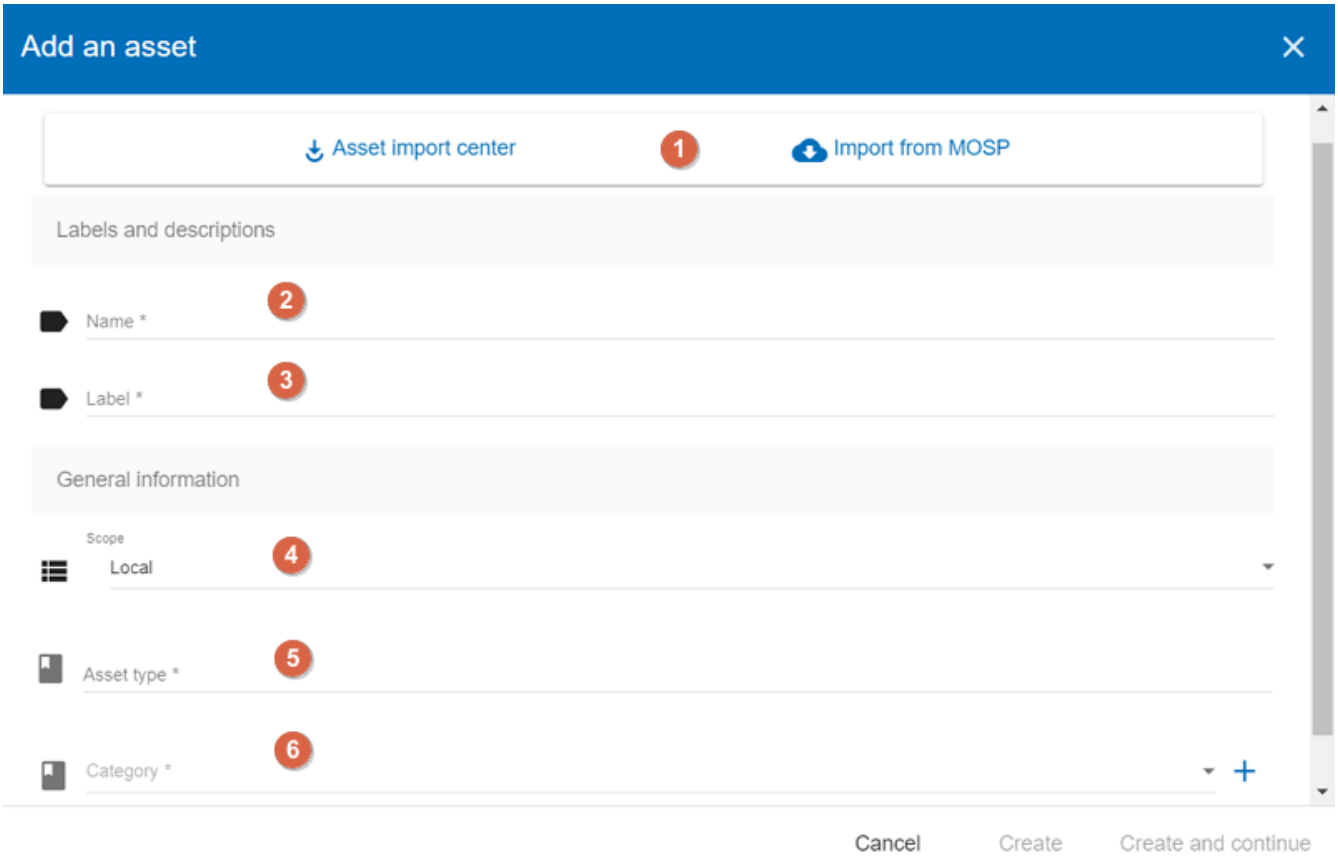


1. Starts the pop-up that allows you to modify most of the parameters of an asset (see Edit an asset).
2. Create a copy of the asset named `Name (copy #)`, which is then renamed with the `Edit Asset` option.
3. Launches asset export pop-up (see Exporting an asset).
4. Publish an asset in MOSP
5. Delete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

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

4.4.3. 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). You have two options, you can import assets from the Asset import center, or MOSP.
2. `Name`: This name must be unique for the analysis.
3. `Label`: This is an additional description, it is displayed in the tooltip when you hover your mouse over an asset.
4. `Scope`: Two possible choices:
   1. `Local`: Identified asset risks are to be assessed whenever the asset is present in the analysis. A primary asset is generally local in scope.
   2. `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 the IT room or main building, once the risks are 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 the risk model associated with it.
6. `Category`: It is the location of the Library where the asset is stored. By clicking on the + sign, a new category can be created.
7. `Operational risk Tag`: It allows the asset to be associated with operational risks by default.

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

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

4.4.4. Edit an asset

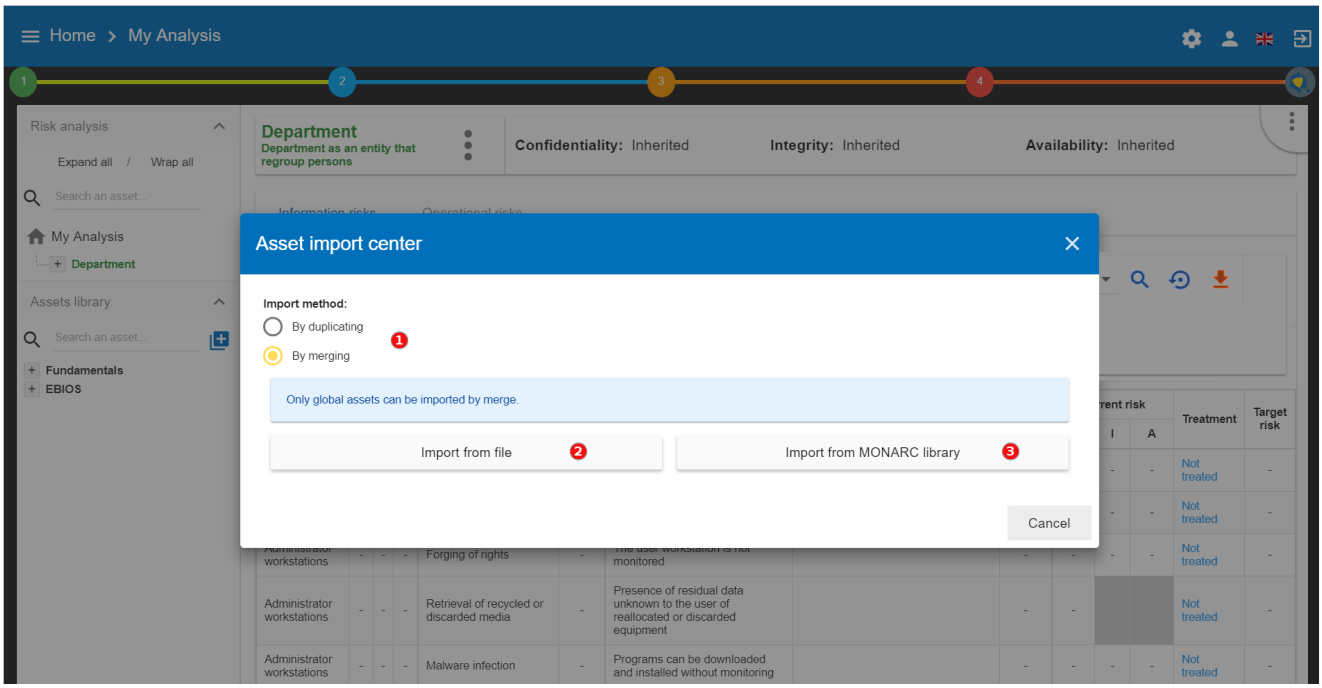
An asset can be edited in the Context menu of the Library (when the asset is selected in the Library).

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`

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

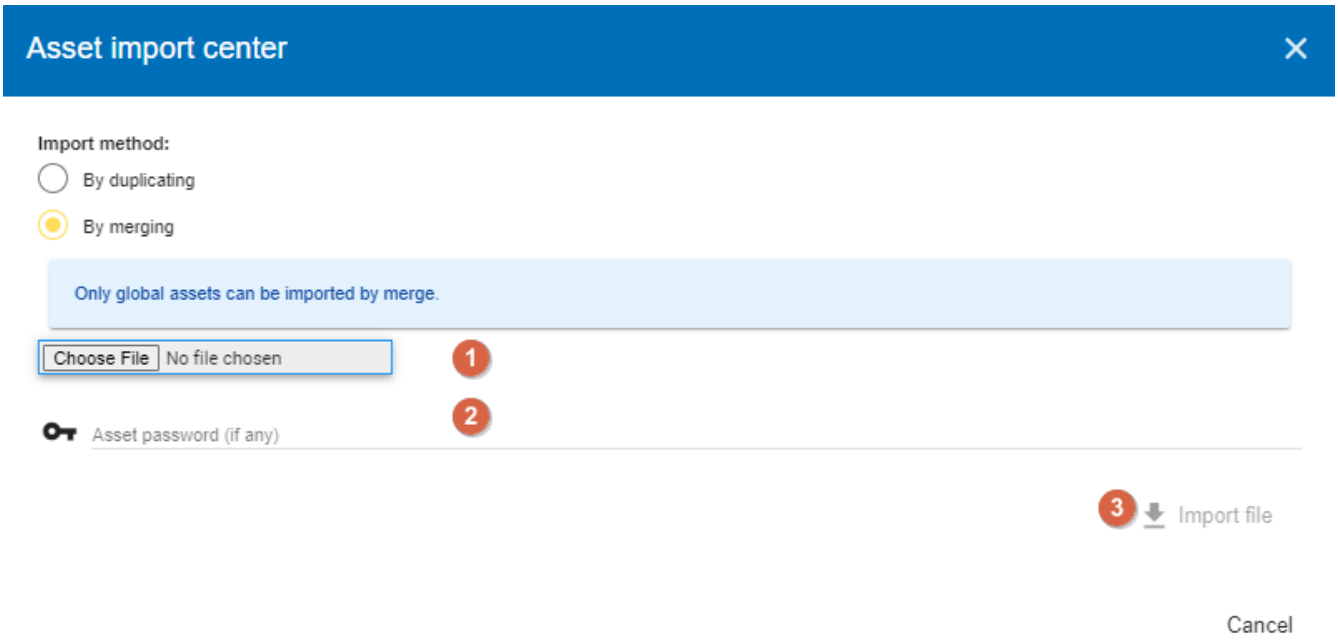
   > Only global assets can be imported by merging.

2. `Import from file`: This allows the transfer of 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`.

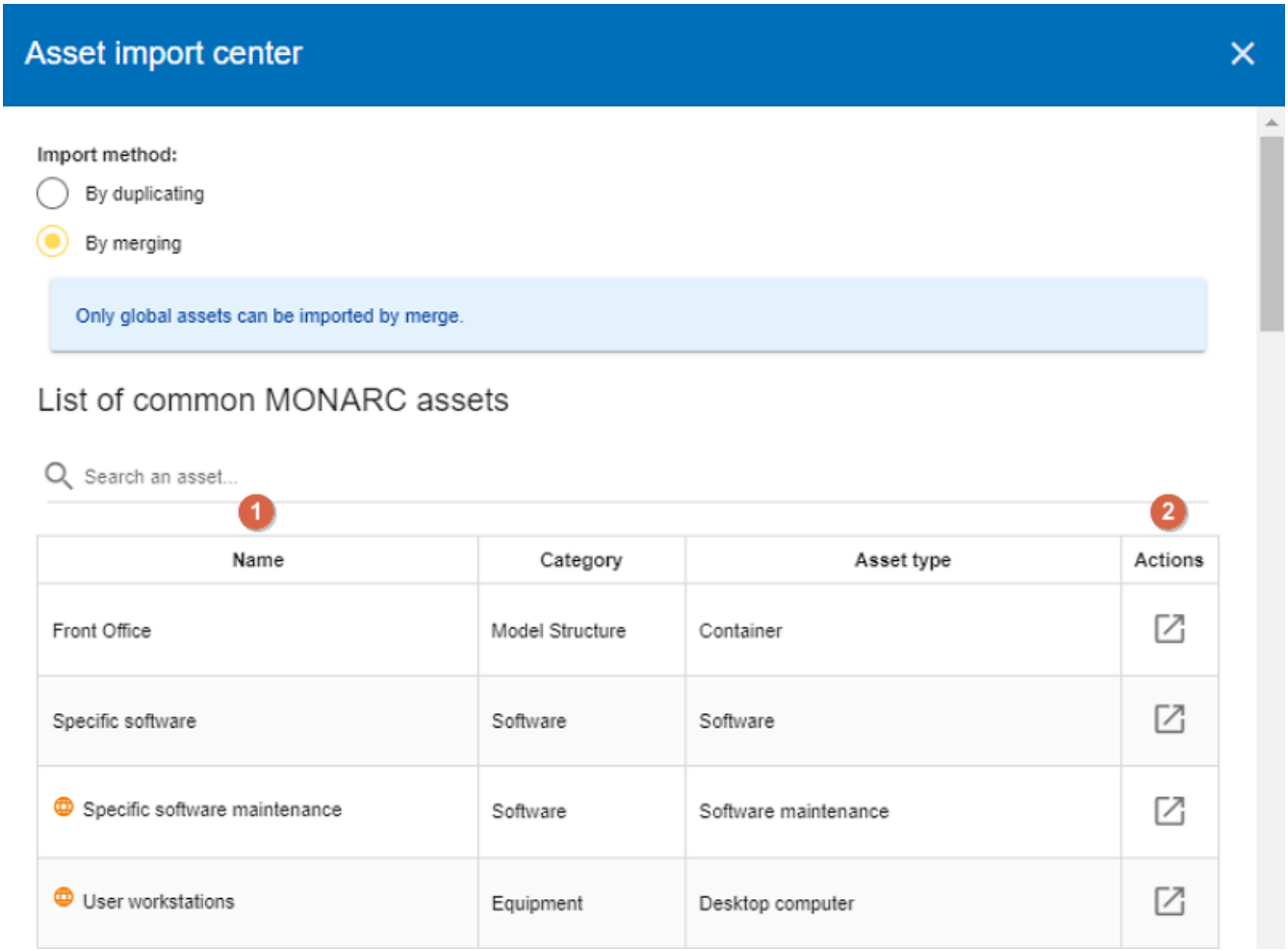


1. `Choose File`: Access the directories of the computer to point to a file.
2. `Asset password`: When exporting the selected file, a password is used to encrypt the file. Please enter the password to be used here.
3. `Import file`: Starts importing a file.

Import from the MONARC Library

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

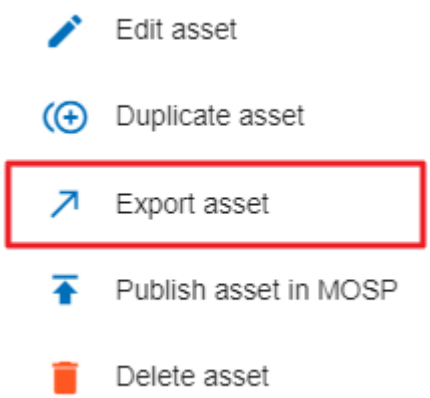
1. Click the + icon (Add an asset)
2. In the Add an asset window, choose the option ‘Asset import center’.
3. Choose MONARC Library



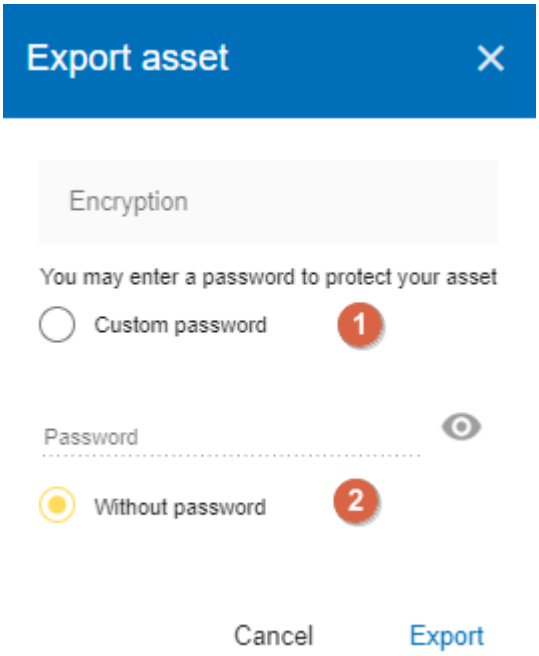
1. Table of available assets in the MONARC common Library.
2. `Action`: Initiate the import procedure for the corresponding asset.

4.4.6. Exporting an asset

To export an asset, click on the asset you want to export. Then click the `Asset management context menu` and choose the option ‘Export asset’:



The ‘Export asset’ window opens where you can decide whether you want to export your asset with a custom password or without a password.

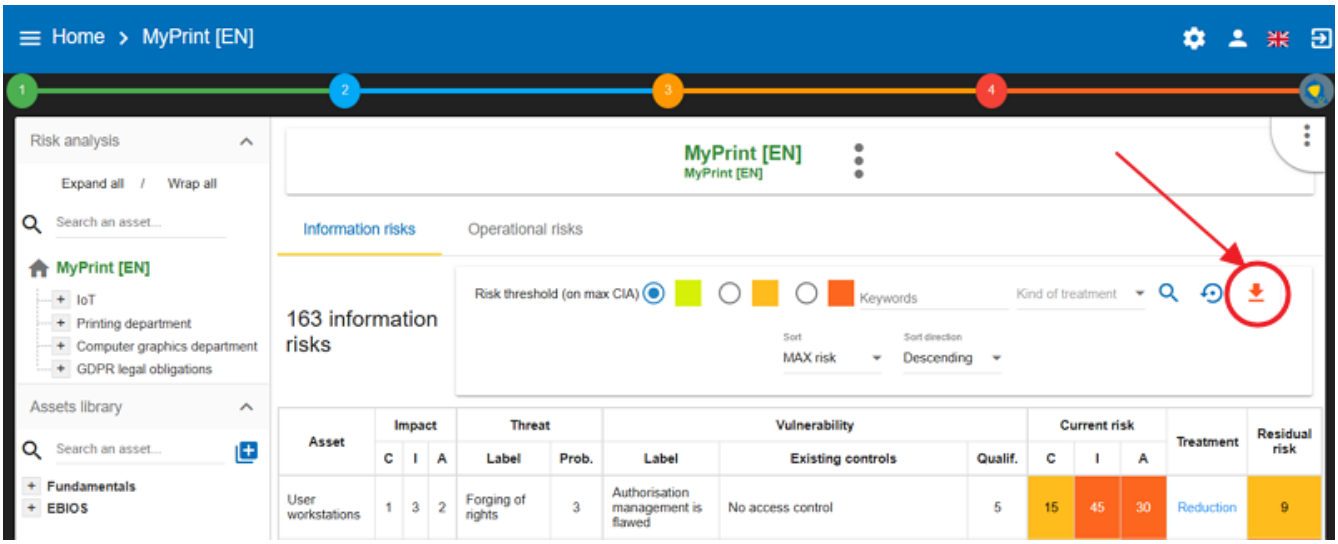


1. `Custom password`: Option to encrypt the generated JSON file with a symmetric password, which is required during the import.
2. `Without password`: If you choose this option, the JSON file will not be encrypted.

Please note that you can export the whole Assets Library.

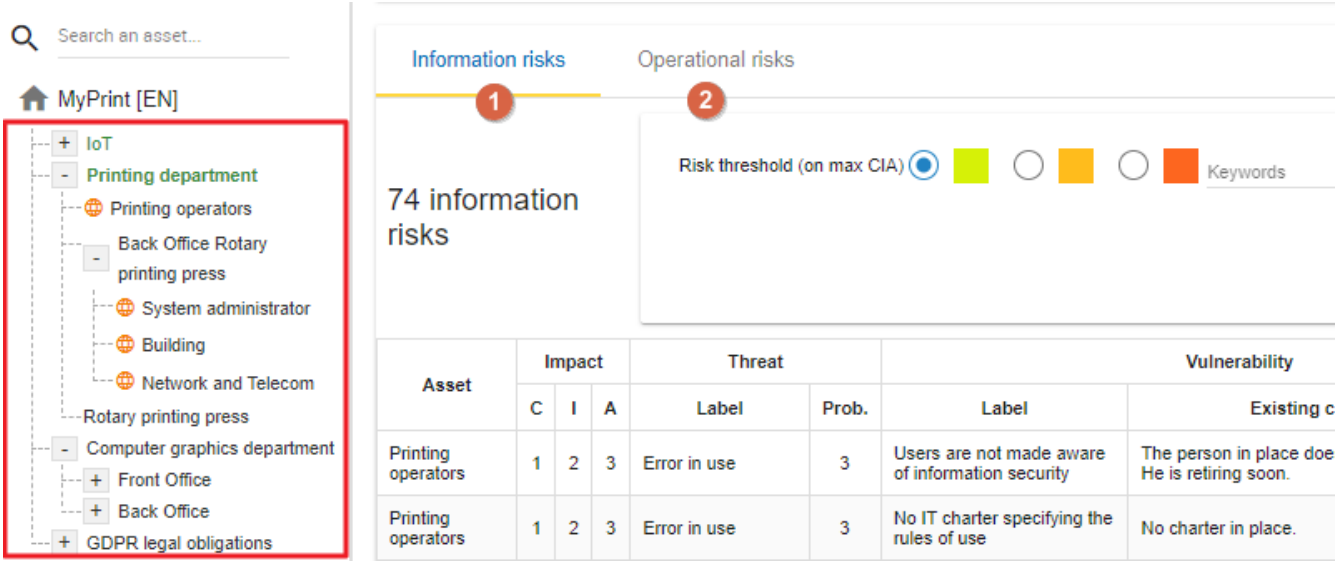
It allows to export (and therefore later import) the complete structure of the Library Assets. This is a very useful feature if you want to share the prepared Assets modelings of analysis. The Assets Library can be exported along with analysis data and Knowledge Base or not.

To export the whole Assets Library, please click on the downward pointing orange arrow (circled in the below screenshot). If you hover your mouse over this icon, the tooltip 'Export (CSV)' appears.



4.5. 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:

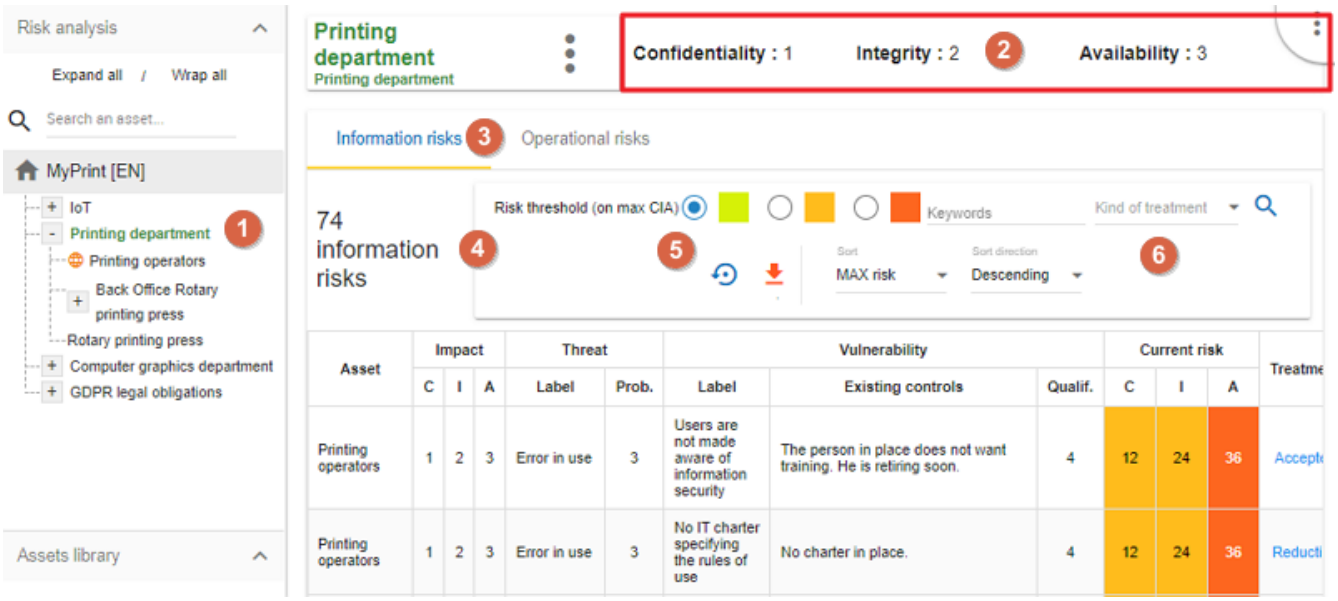


1. The information risk table is based on CIA[1] criteria.
2. The operational risk table is based on ROLFP[2] (see Operational Risks)

Depending on your 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 its supporting assets	Risks associated with themselves
Supporting Asset	Risks associated with themselves	No risks

4.5.1. Risks table



ISO 27005:2022 adaptation

The information risk table now includes a read-only `Risk source` column after `Asset`. It shows the selected source label for each risk or `-` when no source has been assigned yet.

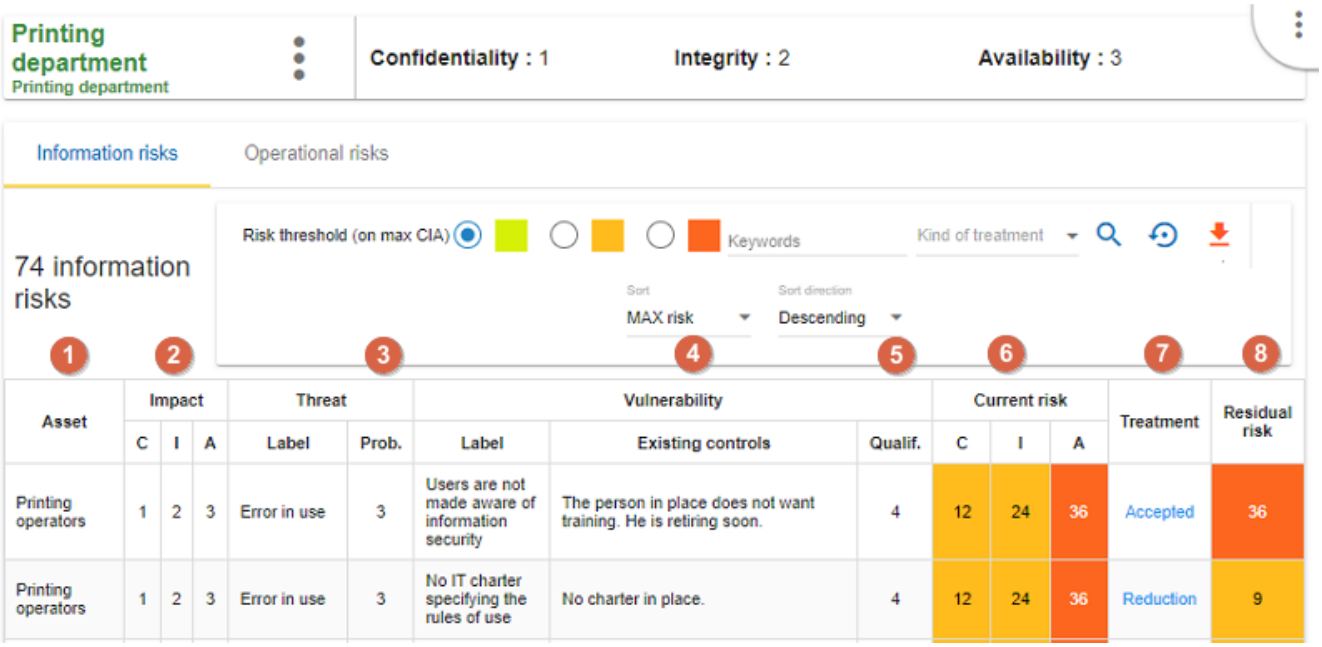
Information risks Operational risks

84 information risks

ID	Asset	Risk source	Impact			Threat
			C	I	A	Label
3913	Employees	-	2	2	3	Error in use
3846	Building	Internal accidental user	4	3	3	Theft or destruction of media, documents or equipment
3868	Administrator workstations	-	-	-	-	Forging of rights
3869	Administrator workstations	Natural event	-	-	-	Forging of rights
3870	Administrator workstations	-	-	-	-	Forging of rights
3875	Administrator workstations	Supplier / third party	-	-	-	Retrieval of recycled or discarded media

1. The primary asset `Printing Department` is selected in the analysis.
2. Display the CIA impacts on the `Printing Department`.
3. Information Risk tab selected.
4. `Department` asset includes supporting assets that collectively provide information on total risks.
5. Possibility to select only certain risks according to the risk acceptance threshold.
6. Ability to sort of most columns of the table.

The risk table consists of the following columns:



1. `Asset`: Assets involved in the evaluation.
2. `CIA Impact`: The CIA criteria that have been assigned to the `Printing Department` are inherited by default from the supporting assets.
3. `Prob`: Likelihood of threat (see Likelihood scale).
4. `Existing controls`: Describes the security control implemented to address the specific vulnerability or, more broadly, the associated 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`: Indicates if the risk is treated or not. It links directly 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 maximum risk because it is not yet treated.

ISO 27005:2022 adaptation

When the risk's `Next reassessment date` is in the past, MONARC displays an orange warning icon next to its identifier. Hover the icon to see the overdue date. The warning is based on the explicit next reassessment date; it is not a risk-level calculation from `Review frequency` alone.

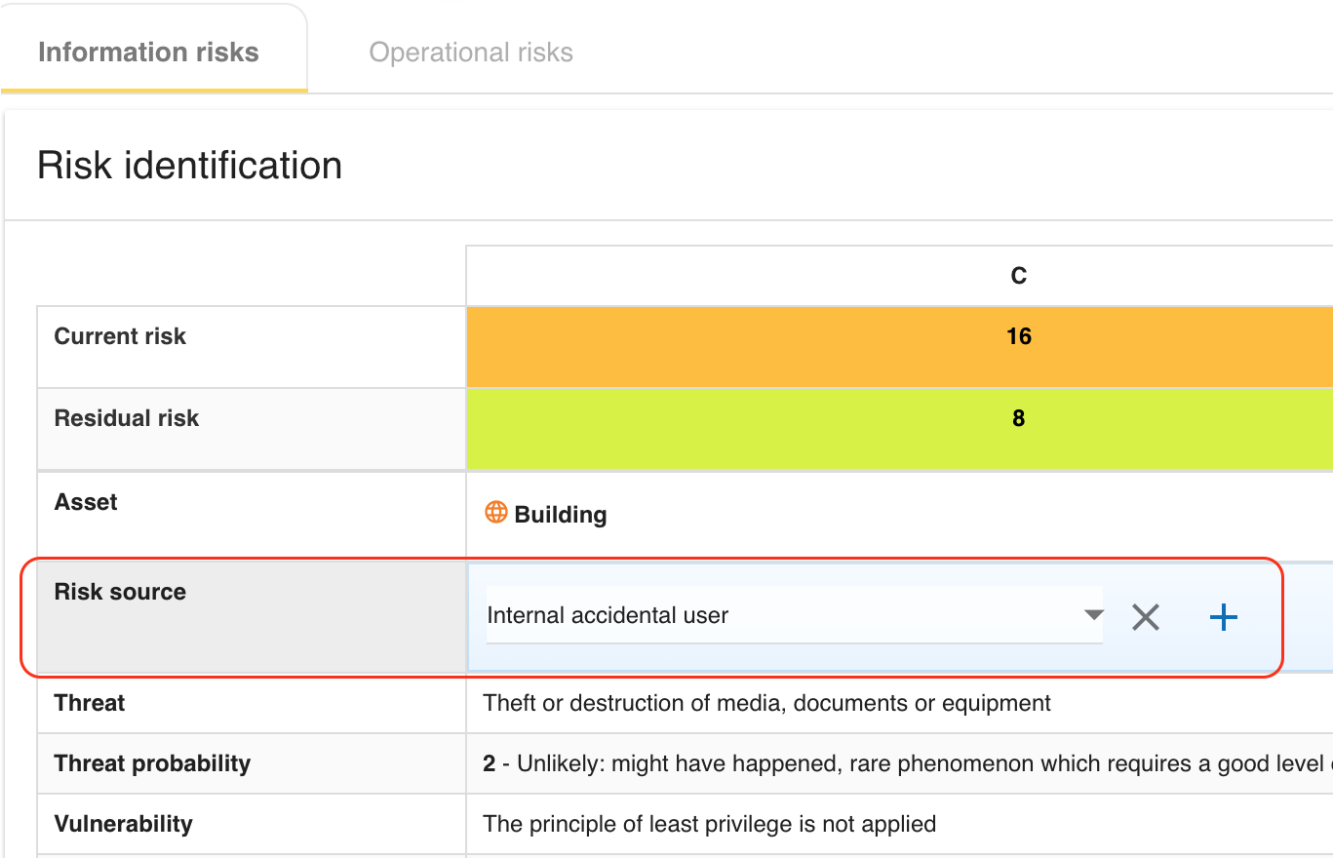
By hovering the cursor over the fields, a relevant tooltip appears.

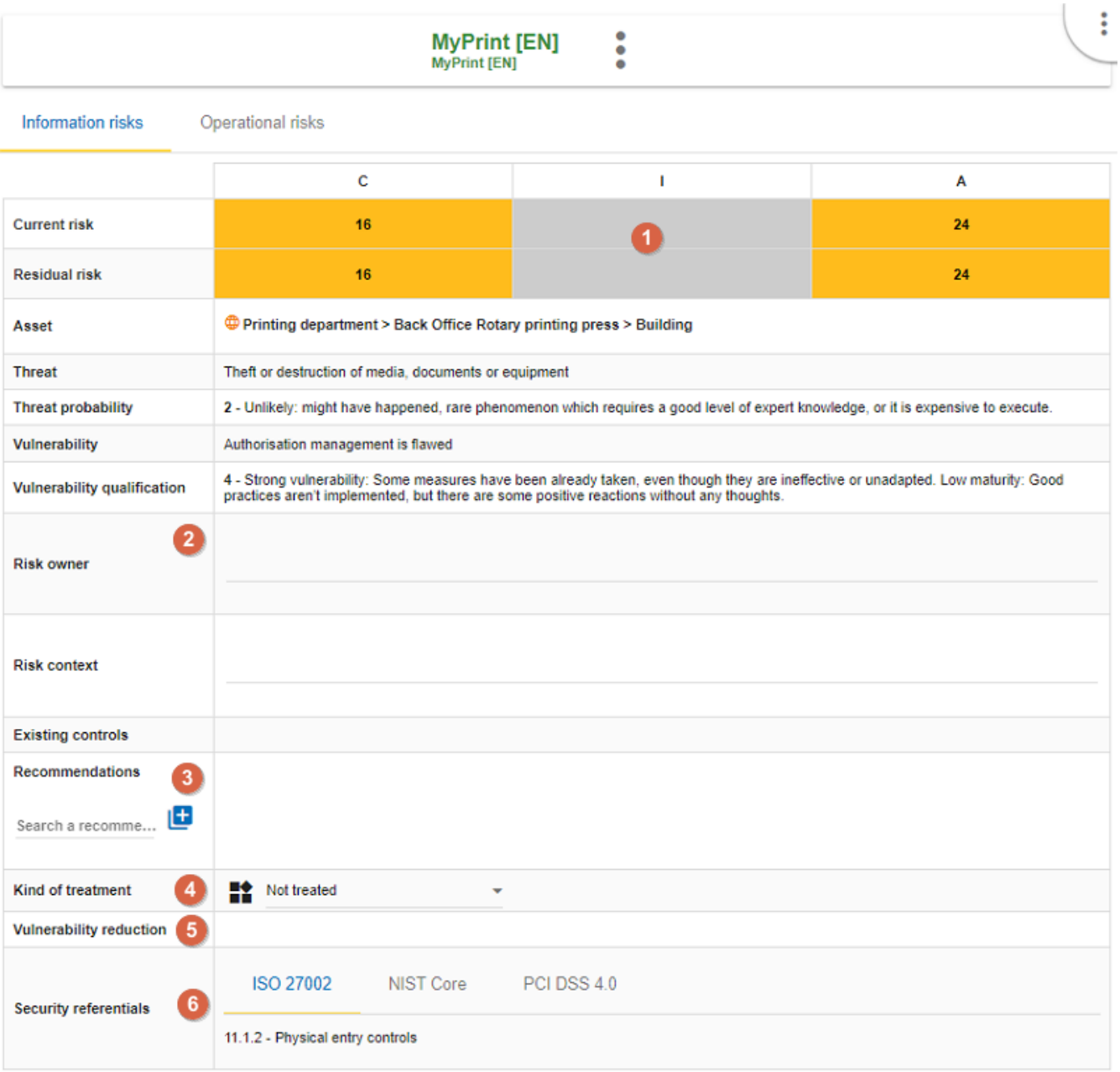
4.5.2. Risk information sheet

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

ISO 27005:2022 adaptation

The information risk sheet now includes a `Risk source` row above `Threat`. From this field, you can select an active source, choose `None`, clear the current value, or create a new source directly from the sheet and assign it immediately.





1. Risk values for CID criteria (not yet covered in the example).
2. Reminders of the parameters of the risk table.
3. Creation / Assignment button for one or more recommendations.
4. Selection of the kind of treatment:
   - Reduction/Modification
   - Denied
   - Accepted
   - Shared
5. Choosing a risk reduction value, the more effective the control is, the greater the reduction value is.
6. Proposals of controls, which come from various repositories.

Do not forget to save the form in order to calculate the residual risk.

ISO 27005:2022 adaptation

The information risk sheet is now organised into dedicated cards:

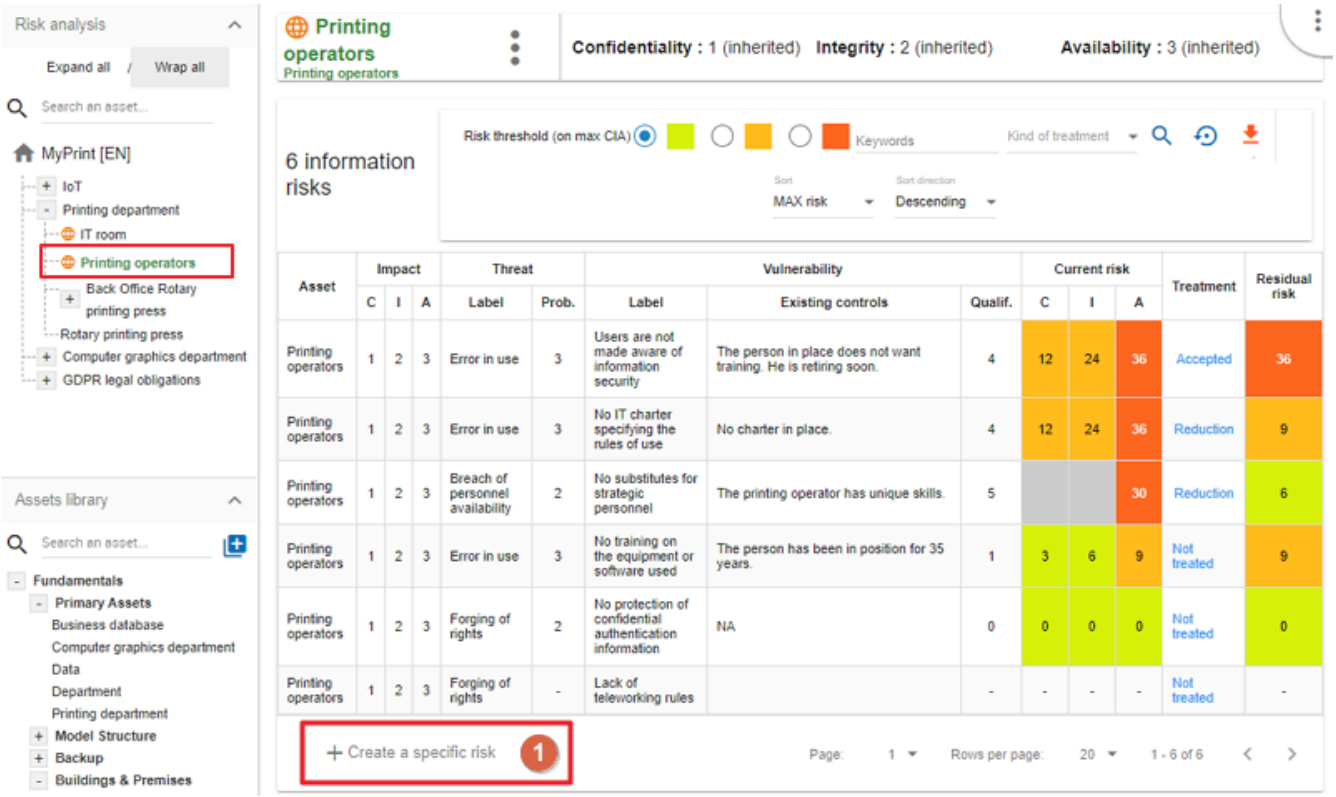
- `Risk identification`
- `Governance & review`
- `Treatment`
- `Residual acceptance`
- `History`

The `Governance & review` card groups the supervisor-based `Risk owner` field with `Last review date`, `Next reassessment date`, `Related reassessment trigger criteria`, and `Review frequency`. Set a last review date to automatically prefill the next reassessment date to one year later. You can retain that date or select another date. A related trigger criterion can be selected only after a next reassessment date has been set; select one or more criteria to show which analysis-level triggers apply to this risk.

The available risk-level review-frequency values are `Monthly`, `Quarterly`, `Semi-annually`, `Annually`, `On trigger`, and `Other`. `Other` accepts a custom label. The review frequency documents the intended rhythm; the overdue warning for a risk is driven by the next reassessment date. The `Residual acceptance` card records the approver, decision, date, performer, and justification of the residual-risk decision after treatment. The `History` card provides a read-only audit trail of changes for the current risk.

4.5.3. Adding additional risk

The below screenshot shows an asset selected in the analysis:

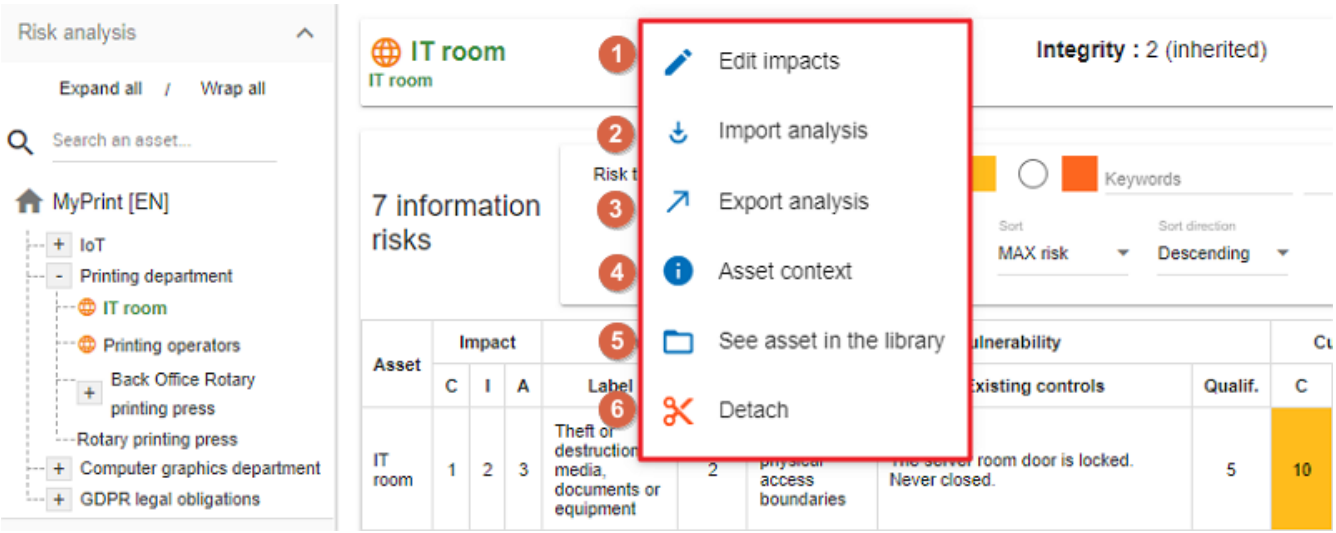


1. Click to `create a specific risk`: A pop-up appears and allows you to associate a threat and vulnerability pair with the current asset.

> Threat and vulnerability must exist beforehand. The risk source can then be assigned afterward from the risk information sheet.

4.5.4. Contextual menu of asset

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

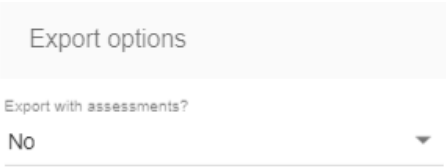


1. `Edit impacts`: Displays the impact and consequence modification view (see Impacts and consequences).
2. `Import analysis`: By clicking on this option, the Asset import center window opens, where you can decide whether you want to import an asset by duplicating or merging it into the analysis

(See Importing an asset.). You can choose a file and give a password to the import.

3. `Export analysis`: This option 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, is `export with assessment`. It means, export gets the evaluation and treatment of risks. By default is disabled.



4. Asset context: The Asset context window opens, where you can add asset context fields (labels) to the asset. Each asset can have custom context set by clicking on the 3 dots of the asset context menu. The labels of the context field values are created on the analysis wise and the values of the context are particular to the selected asset. If an asset is global the context value is shared to its siblings.

You can add asset context fields by clicking on the + icon at the bottom of the popup. You can edit the field label by clicking in the pencil icon or delete it by clicking on the trash bin icon:

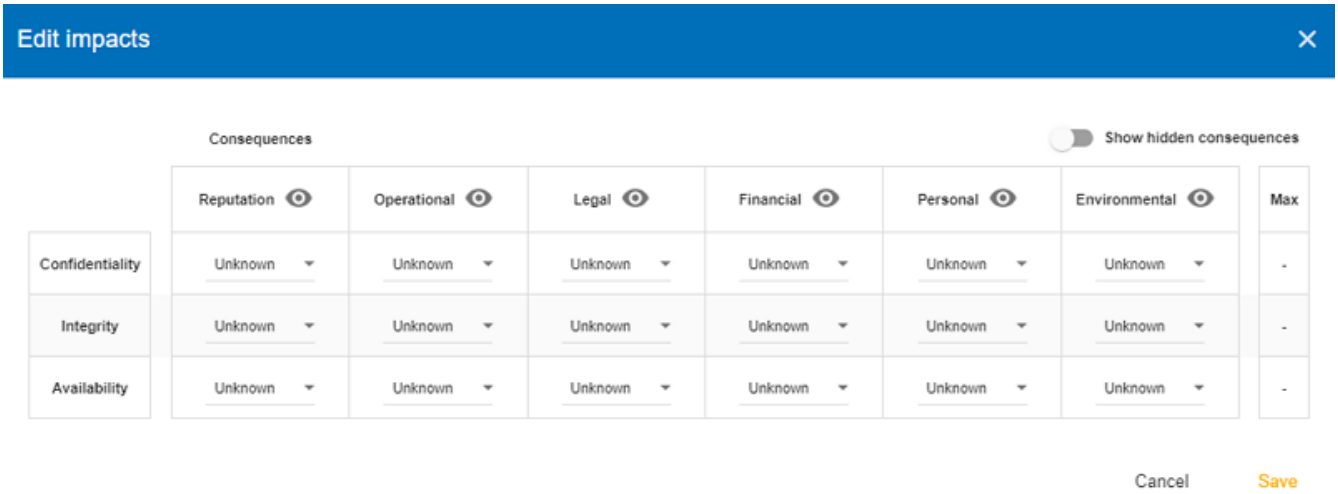
5. `See asset in the library`: Displays the asset from the library, allowing you to have another context menu that allows changes to the asset. (See the [Context menu of library].)
6. `Detach` : This option removes an asset from the risk analysis.

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

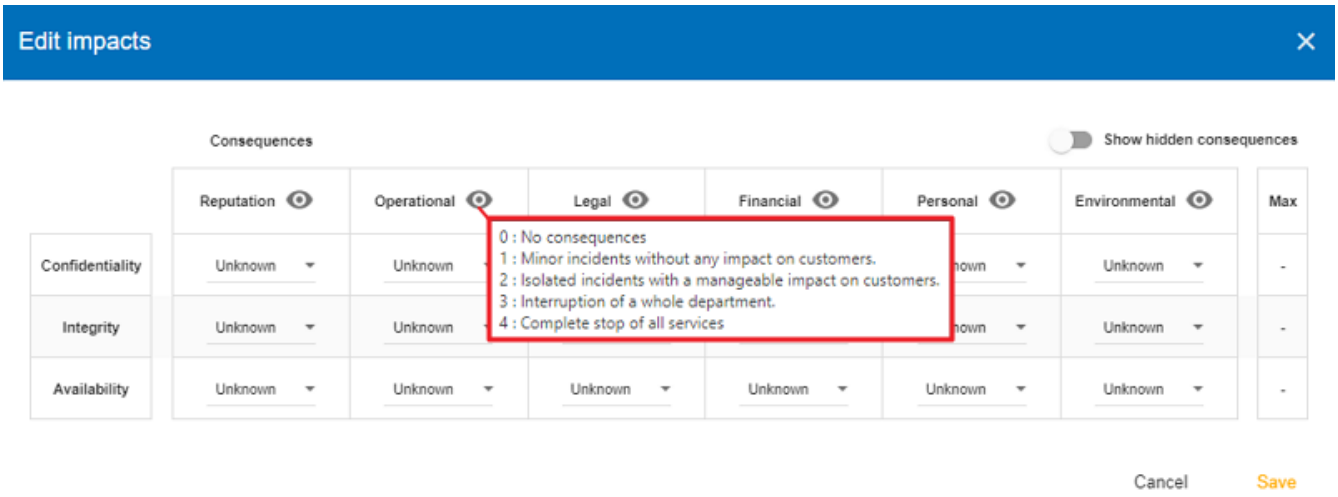
4.5.5. Impacts and consequences

Edit impacts

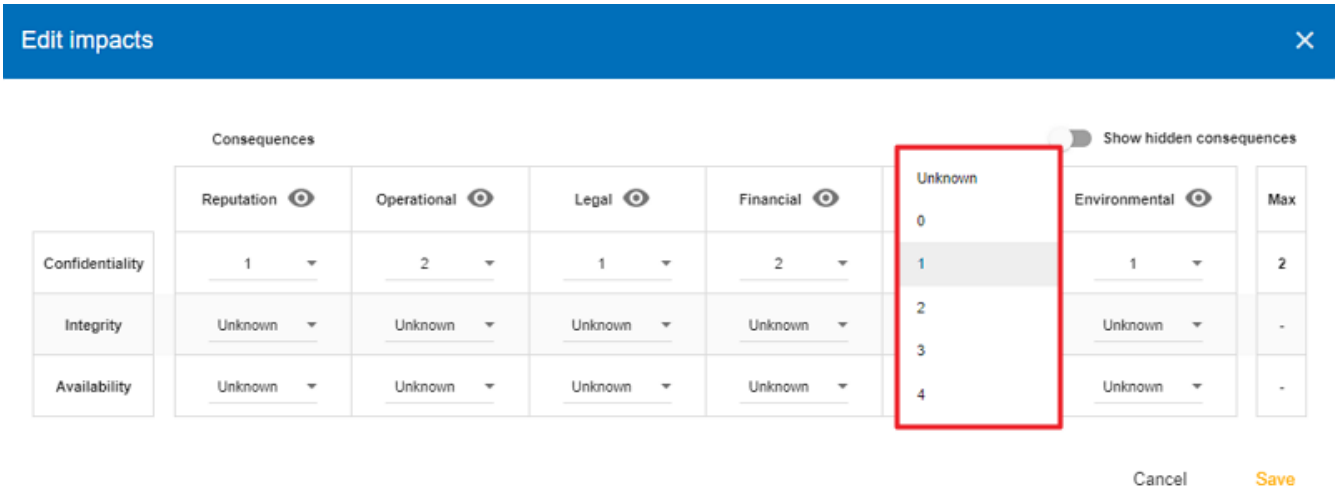
The first contextual menu of an asset is called the ‘Edit impacts’. The goal is to determine the level of primary assets and assess the potential impacts and consequences that may arise from the realization of the model’s risks. Once you click on the ‘Edit impacts’ link, the following pop-up appears:



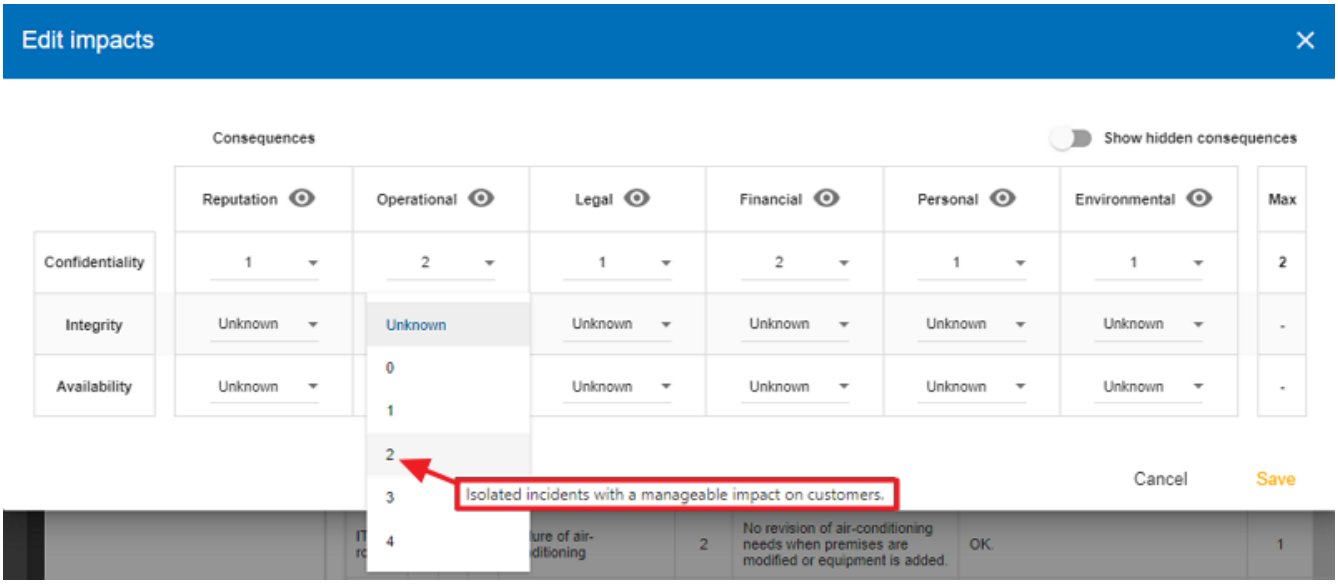
When you hover your mouse over the eye-shaped icon next to the column names, a relevant tooltip appears. For example, hovering over the 'Operational' column will display the following tooltip:



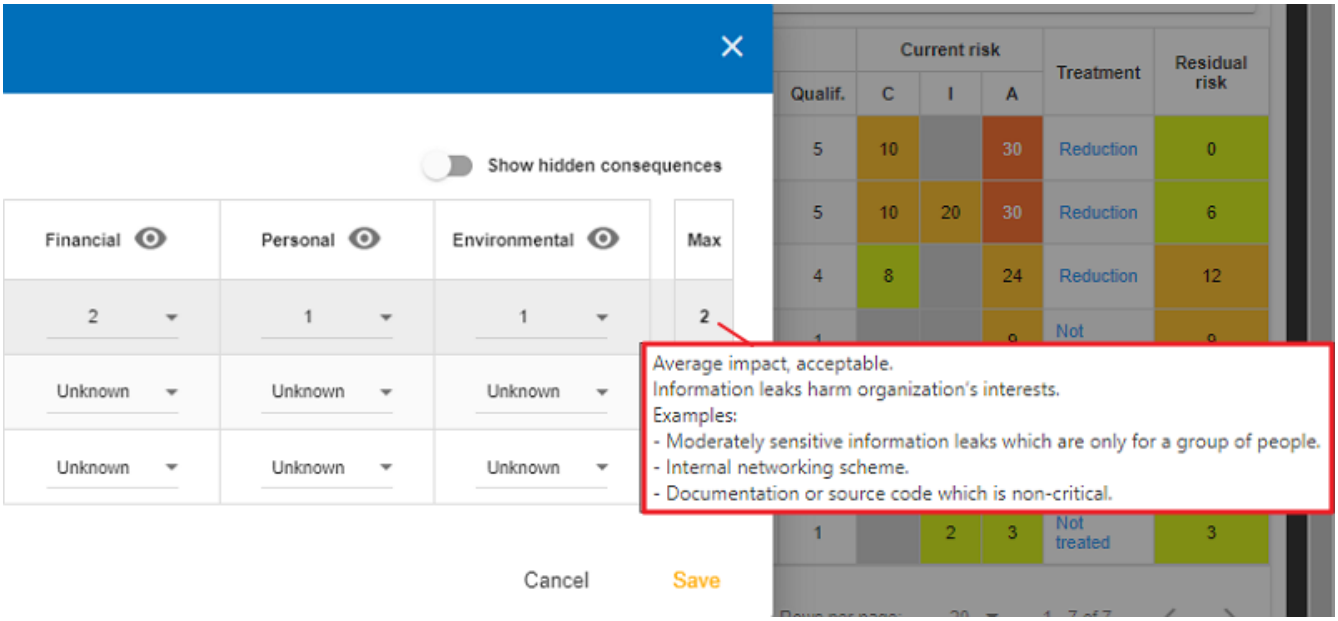
Next, set the consequences (e.g., Reputation, Operational, etc.) based on the aspects of Confidentiality, Integrity, and Availability by selecting the appropriate value (0, 1, 2, 3, or 4) from the drop-down menu:



The tooltips always help you. For example, hover your mouse over the value 2 to see the consequence it describes for the 'Operational' consequence under the 'Integrity' aspect:



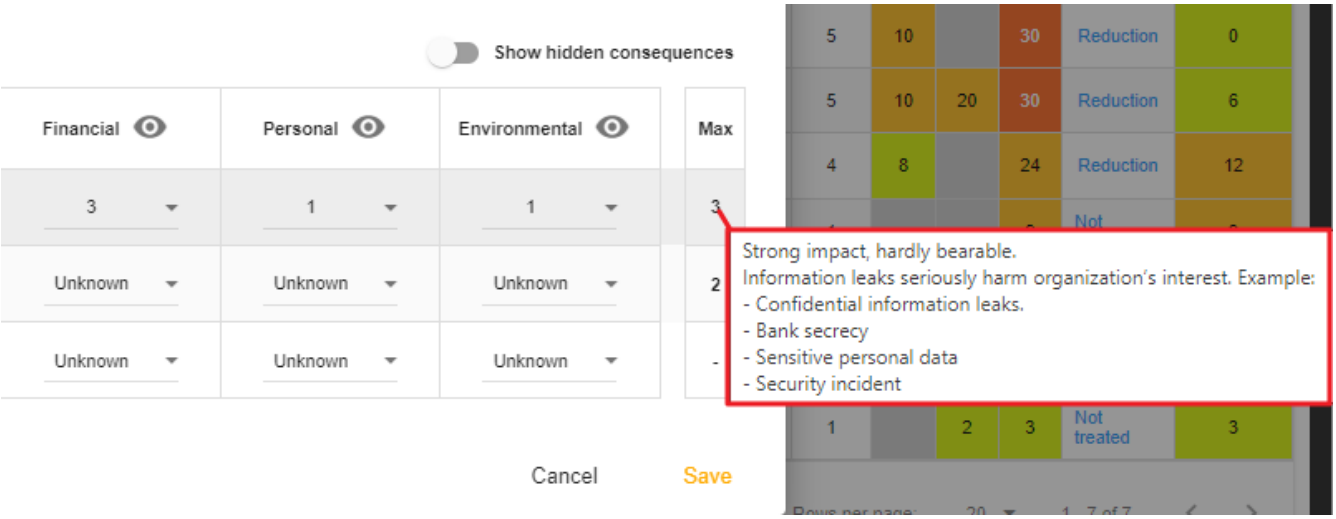
These tooltips help a lot in choosing the right values. If you have selected the values everywhere, it is worth reviewing the values on the right side of the table (there are also tooltips here).



If you find the settings appropriate, save them by clicking on the 'Save' button.

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

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



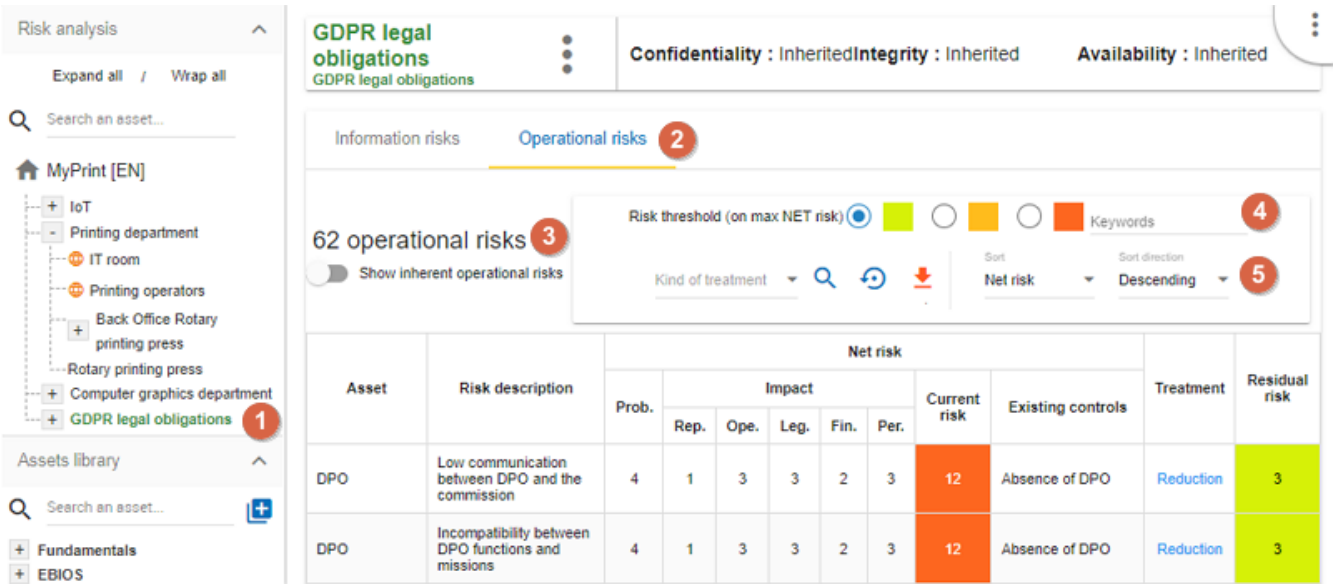
In the case of the above figure, the 3 (out of 5) impact on confidentiality, is explained by the maximum value ROLFP regarding confidentiality. For example, 3 is the consequence of the person in case of disclosure of his personal file.

To hide the consequences that will not be considered. Click on the icon 👁. To show it again. Click on `Show hidden consequences`.

4.6. Operational Risks

4.6.1. Risks table

Below is an example of an Operational Risk table.



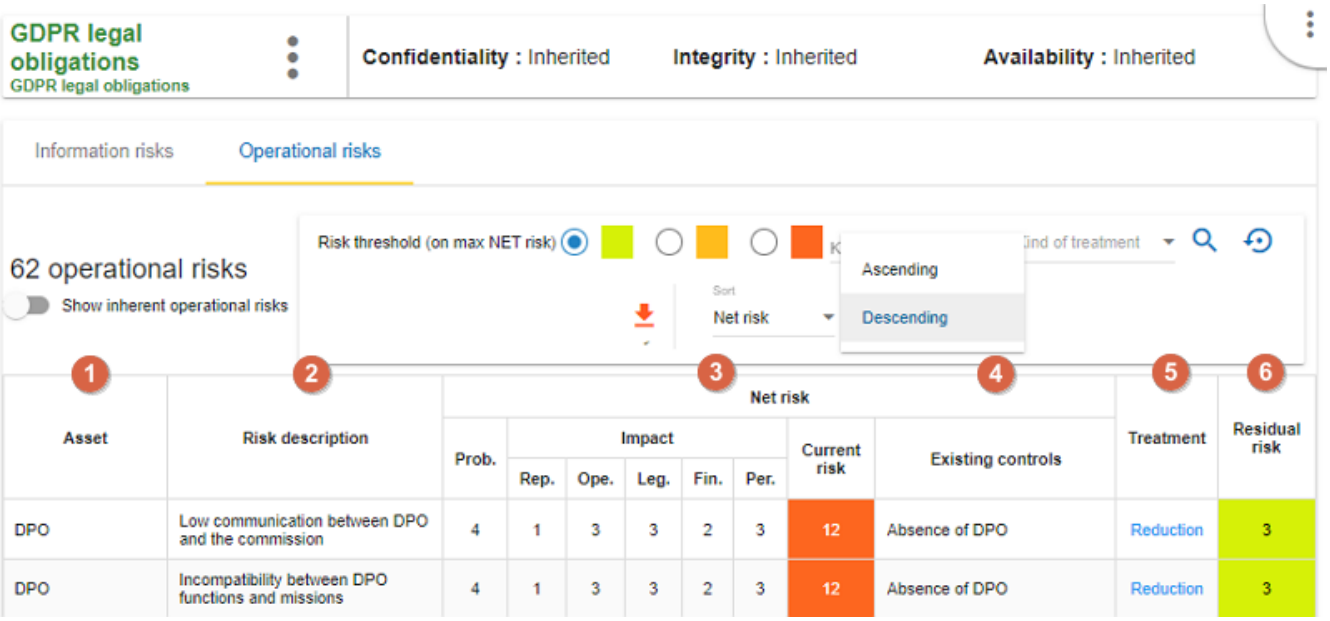
ISO 27005:2022 adaptation

The operational risk table now includes a read-only `Risk source` column between `Asset` and `Risk description`. It keeps the origin of the scenario visible directly in the operational risk register and displays `-` when no source has been assigned yet.

To reach this table, please follow the steps as follows:

1. Select the primary asset. In this case, `GDPR legal obligations`.
2. Click on the tab `Operational risks`.
3. The figure shows the total operational risks associated with the primary asset.
4. By selecting the relevant radio button, you can choose specific risks based on the risk acceptance threshold.
5. Ability to sort most columns of the table. The sort can be done by Asset, Position, Net probability, Net risk, and Residual risk. The sort direction can be Ascending or Descending.

> 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. `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 maximum risk because it has not yet been treated.

ISO 27005:2022 adaptation

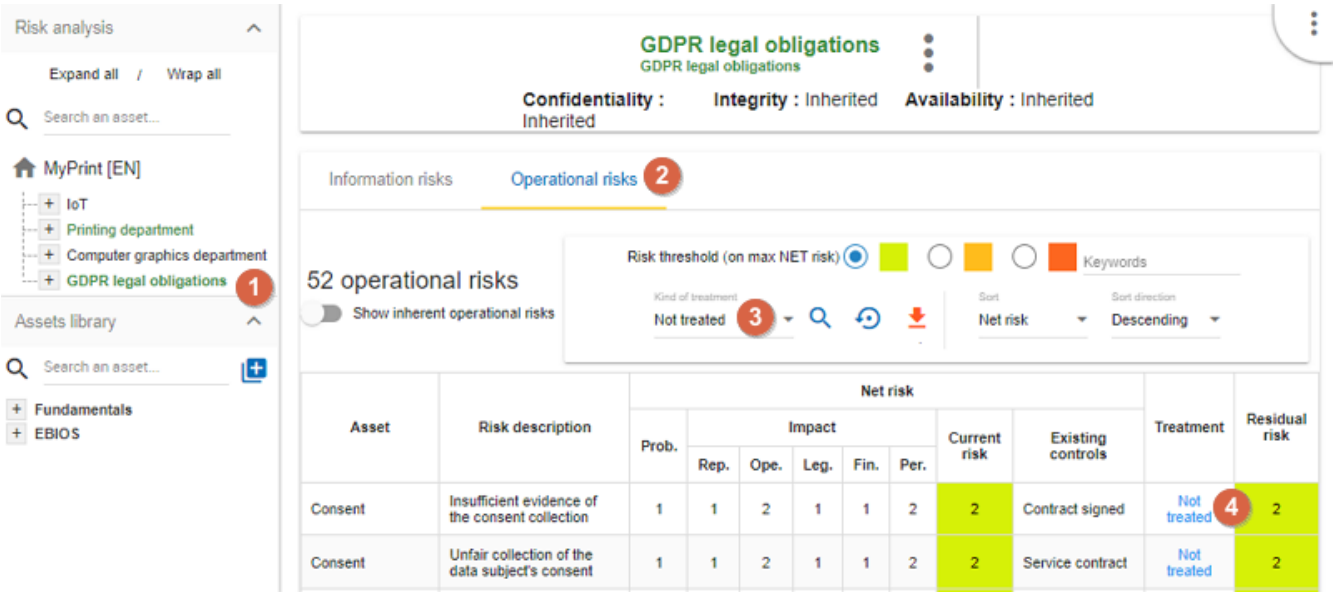
When the operational risk's `Next reassessment date` is in the past, an orange warning icon is displayed next to its identifier. Hover the icon to see the overdue date.

4.6.2. Operational risk sheet

In the risk analysis, click on an asset and choose the Operational risk tab. Then, in the 'Kind of treatment' dropdown menu choose 'Not treated'. The not treated assets should appear in the table.

ISO 27005:2022 adaptation

The operational risk sheet now includes a `Risk source` row above `Risk description`. From this field, you can select an active source, choose `None`, clear the current value, or create a new source directly from the sheet and assign it immediately.



Click on the `Not treated` link in the operational risk table, so the risk card is displayed.

GDPR legal obligations
GDPR legal obligations

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

Information risks | Operational risks

	Prob.	Impact					MAX risk
		Reputation	Operational	Legal	Financial	Personal	
Current risk (1)	1	1	2	1	1	2	2
Residual risk (2)	1	1	2	1	1	2	2
Asset (3)	Consent						
Risk description (4)	Insufficient evidence of the consent collection						
Risk owner (5)							
Risk context (6)	This is a free text field.						
Risk probability	1 - Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.						
Existing controls	Contract signed						
Recommendations (7) Search a re...							
Kind of treatment (8)	Not treated						
Security referentials (9)	ISO 27002 NIST Core PCI DSS 4.0						

Previous Back to the list Next

1. `Current risk`: Values for risk probability (`Prob.`) and ROLFP[4] Criteria.
2. `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. Reminders of the parameters of the risk table.
3. `Asset`: the name of the asset
4. `Risk description`: the description of the risk
5. `Risk owner` : This field is aligned to the ISO27005 latest specification and allow you to specify the risk owner. The risk owner is saved in the database and can be selected by typing its first letter for using in another risks.
6. `Risk context` : This field is aligned to the ISO27005 latest specification and allow you to specify

the risk context.The context field is a free text field.

7. `Recommmendations` : Creation / Assignment button for adding one or more recommendations.
8. `Kind of treatment` : Selection of the type of risk treatment (Not treated, Reduction, Denied, Accepted, or Shared).
9. `Security referentials` : (ISO 27002, NIST Core, etc.)

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

ISO 27005:2022 adaptation

The operational risk sheet now follows the same card structure as the information risk sheet:

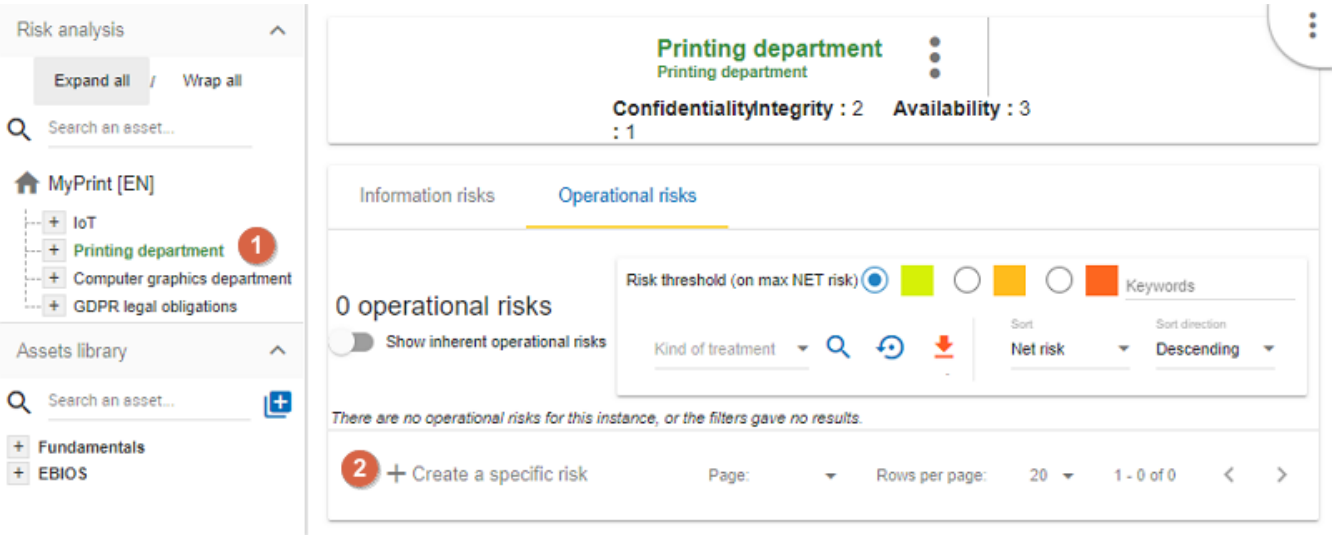
- `Risk identification`
- `Governance & review`
- `Treatment`
- `Residual acceptance`
- `History`

The `Governance & review` card contains the supervisor-based `Risk owner` field together with `Last review date`, `Next reassessment date`, `Related reassessment trigger criteria`, and `Review frequency`. When a last review date is set, MONARC proposes a next reassessment date one year later. You may change that date. Related trigger criteria become available after a next reassessment date is set and link the operational risk to one or more analysis-level trigger criteria.

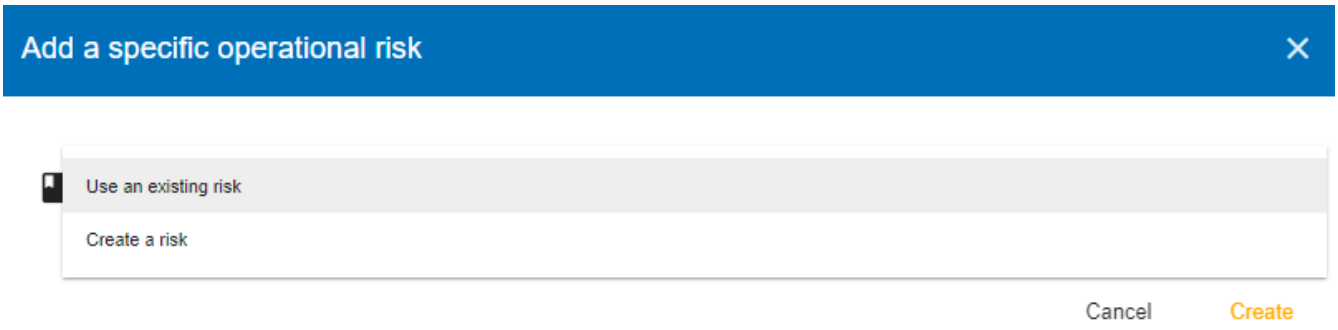
The risk-level review frequency can be `Monthly`, `Quarterly`, `Semi-annually`, `Annually`, `On trigger`, or `Other` with a custom value. It records the intended rhythm; the warning icon is controlled by the explicit next reassessment date. The `Residual acceptance` card captures the residual-risk approver, decision, date, performer, and justification. The `History` card exposes a read-only audit trail for the current operational risk.

4.6.3. Adding additional risk

You can add further risks to your risk table. Select an asset in the risk analysis and click on the ‘Create a specific risk’ link below the risk table:



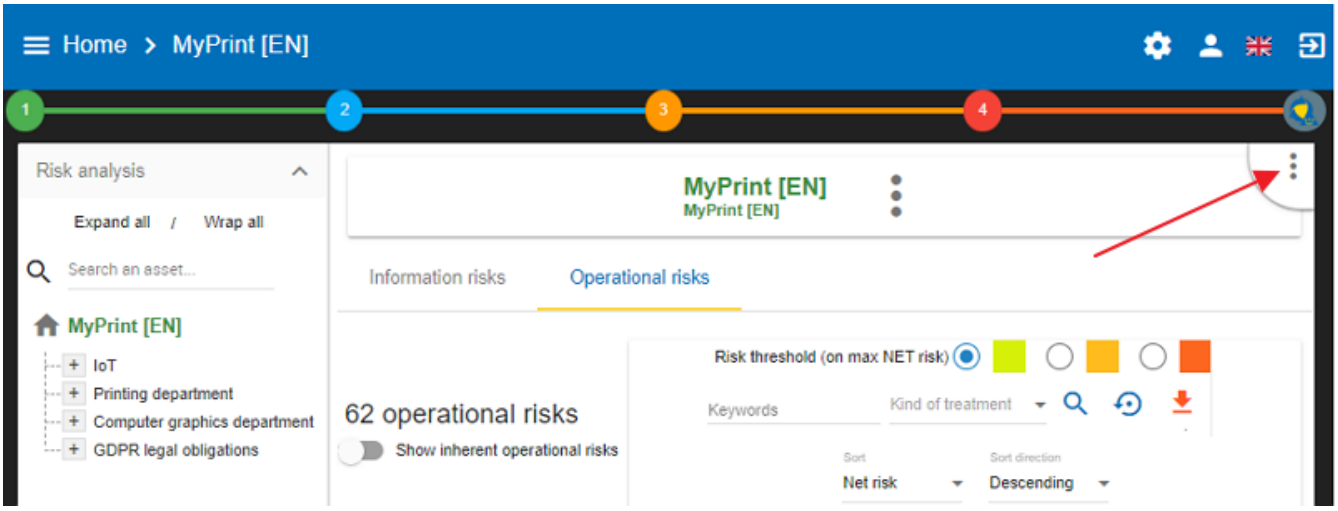
1. Click to `create a specific risk`: A pop-up appears and allows a new risk to be associated with the current asset. If the risk does not exist, it can be created directly. In the popup window, you can decide whether you want to add an existing risk or create a new one:



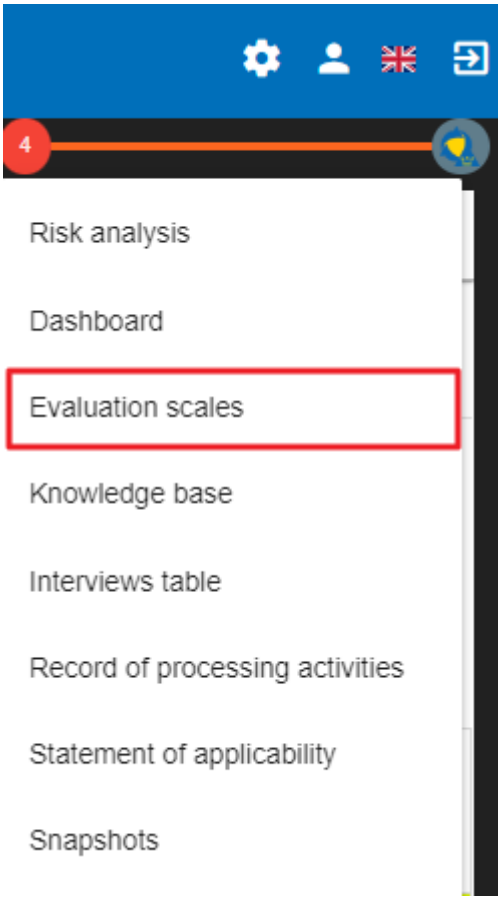
[1] CIA,Confidentiality, Integrity and Availability.
[2] rolfp,Reputation, Operational, Legal, Financial and Personal
[3] rolfp
[4] rolfp
[5] rolfp

Chapter 5. Evaluation Scales

To reach the 'Evaluation scales' menu, use the contextual menu (three-dot menu) in the top right-hand corner of the application.



Once you click on the three-dot menu, a submenu opens. Choose the submenu 'Evaluation scales':



The screen has three tabs as follows:

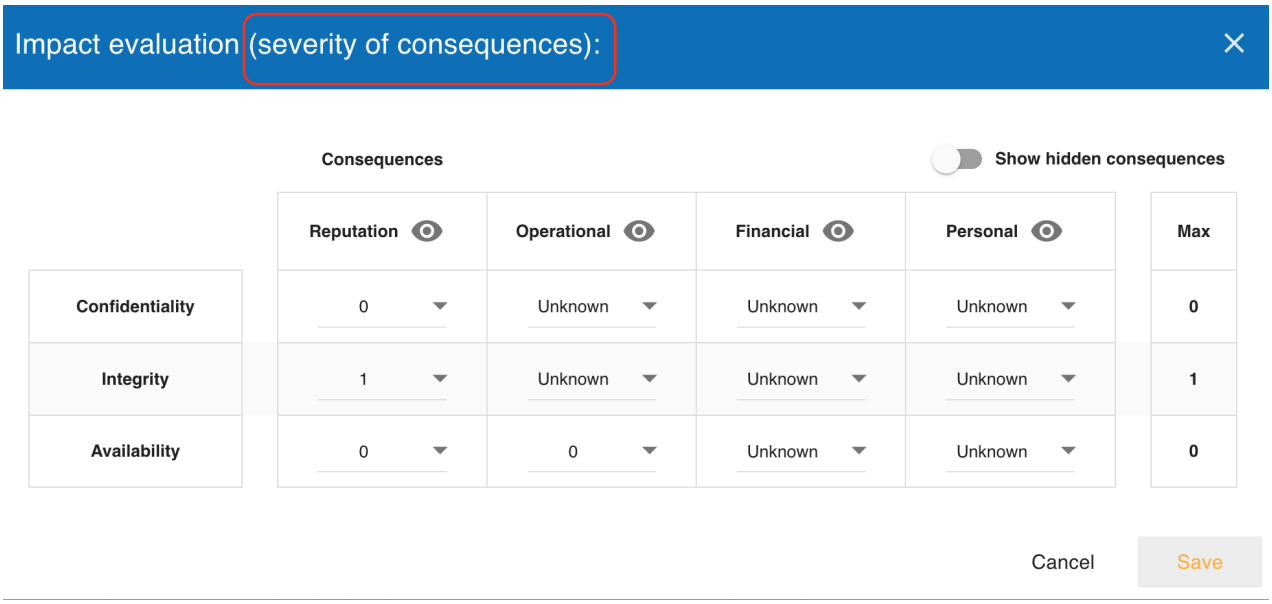
1. Information risks
2. Operational risks
3. Compliance

This chapter is divided into three parts accordingly.

5.1. Information risks

ISO 27005:2022 adaptation

In the current interface, the impact-scale area is labelled `Impact evaluation (severity of consequences)`. This wording clarifies that impact represents the severity of consequences while keeping the same MONARC impact model and calculations.



The `Evaluation scales` window opens which has the following parts (from top to bottom):

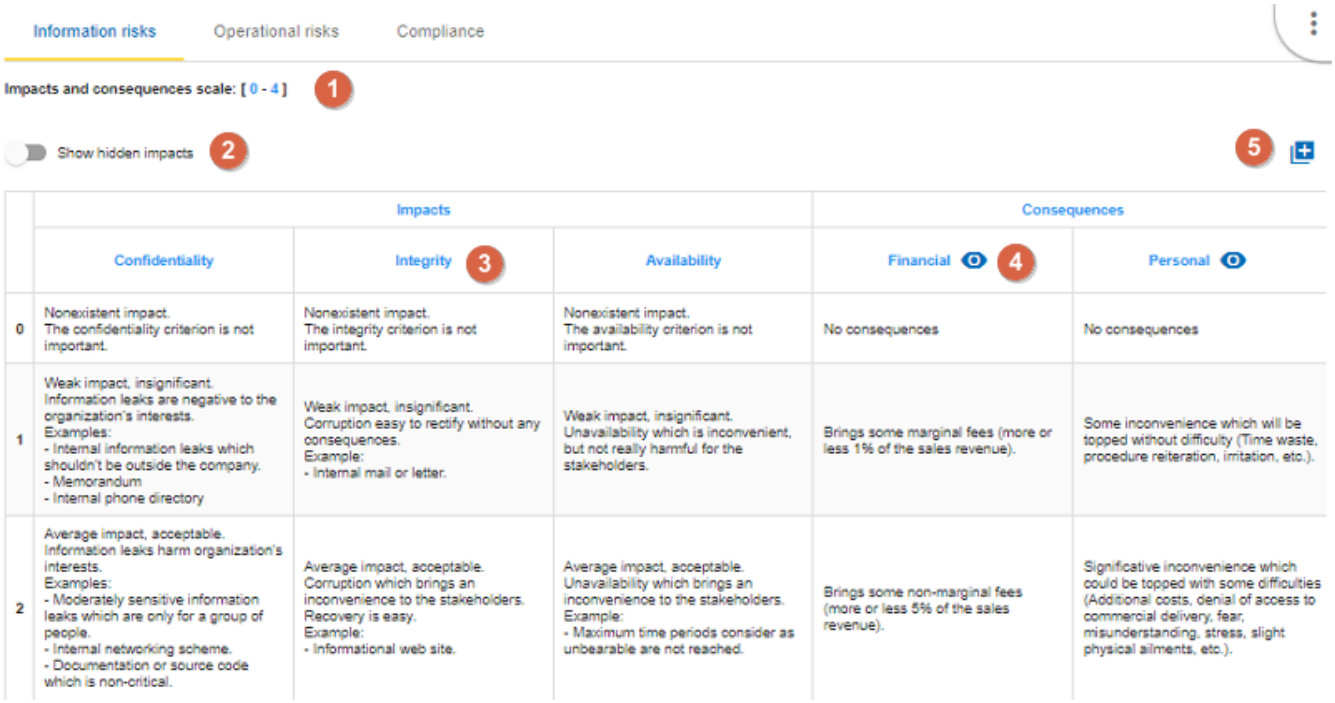
1. Impacts and consequences scale
2. Likelihood scale
3. Vulnerabilities scale
4. Acceptance thresholds of information risks

All scales are editable and customizable.

However, it is no longer permitted to modify scales as soon as an evaluation has been encoded.

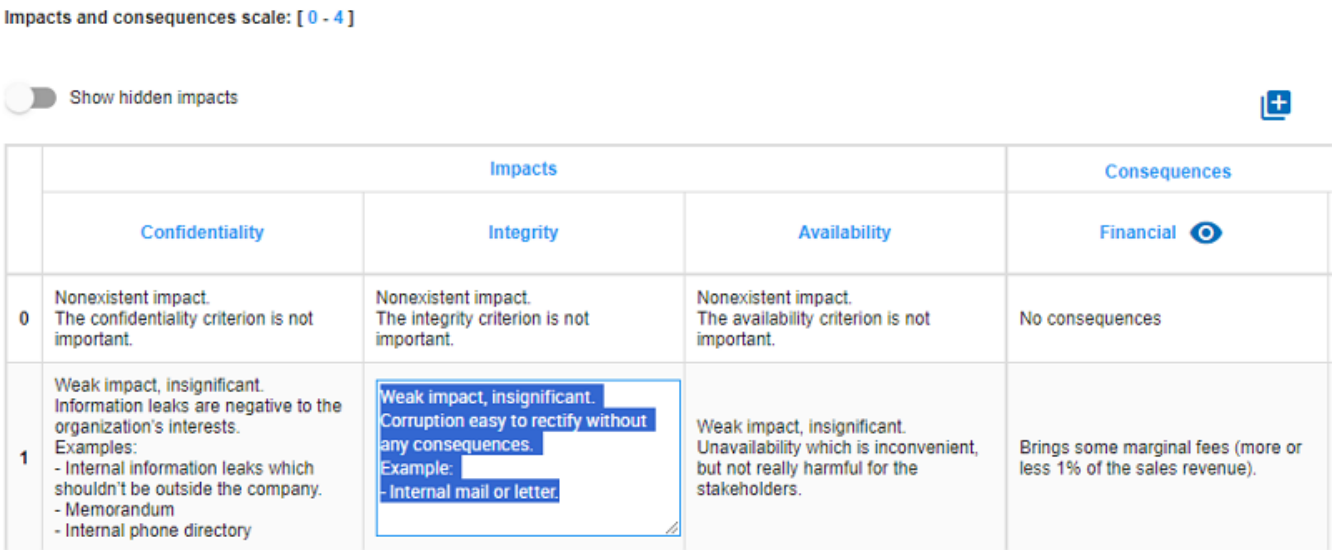
5.1.1. Impacts and consequences scale

The first section of the Evaluation scales window is the 'Impacts and consequences scale' table. It is a fully customizable table, by clicking on its different parts, you can edit it.



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

Please note that you can edit the headings and the content of the cells by simply clicking on them, allowing you to provide different values or explanations.



5.1.2. Likelihood scale

The Likelihood scale is the second part of the window. It is a fully customizable table, by clicking on its different parts, you can edit it. In the below example, there are only five scale values of the scale between 0-4.

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

You can modify it easily. Just click on any of the values and give a different value: the Impacts and consequences scale table will change accordingly.

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

Just like with the scale values, you can also modify the description/explanation of the values by clicking on them and giving a different description/explanation.

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

5.1.3. Vulnerability scale

The third section of the Evaluation scales window is the ‘Vulnerability scale’ table. It is a fully customizable table, by clicking on its different parts, you can edit it.

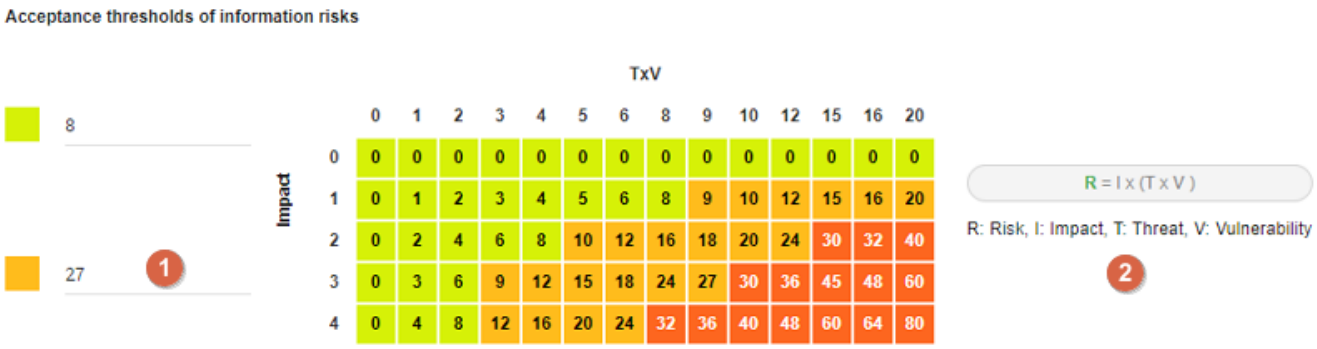
Vulnerabilities scale: [0 - 5] 1

0. No vulnerabilities.
1. Very weak vulnerability: Some efficient measures have been already taken, and their effectiveness is controlled. 2
Very high maturity: Good practices are implemented and frequently verified.
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.

1. Click to modify the number of scales.
2. Click to edit the heading on each scale (Management identical to the impact scale).

5.1.4. Acceptance thresholds

The fourth section of the Evaluation scales window is the ‘Acceptance thresholds’ table. There are two separate tables for acceptability thresholds, as operational risks and information risks are not calculated in the same way. Information risks are calculated using three criteria:



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`.

5.2. Operational risk scales

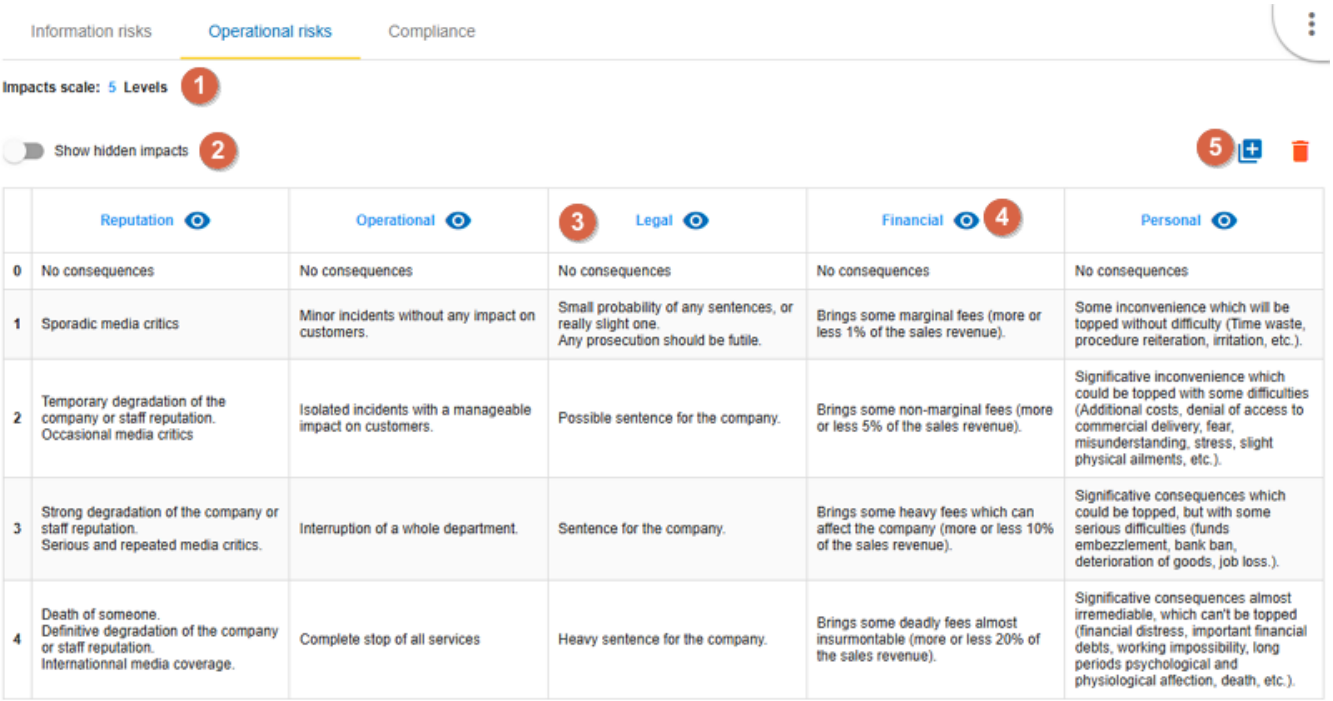
To reach the ‘Evaluation scales’ menu, use the contextual menu (three-dot menu) in the top right-hand corner of the application and choose the submenu 'Evaluation scales'. The Operational risks screen can be reached by clicking on the second tab of the screen 'Operatioanl risks'.

The Operational risks screen consists of three parts as follows:

1. Impact scale
2. Likelihood scale
3. Acceptance threshods of operational risks

5.2.1. Impact scale

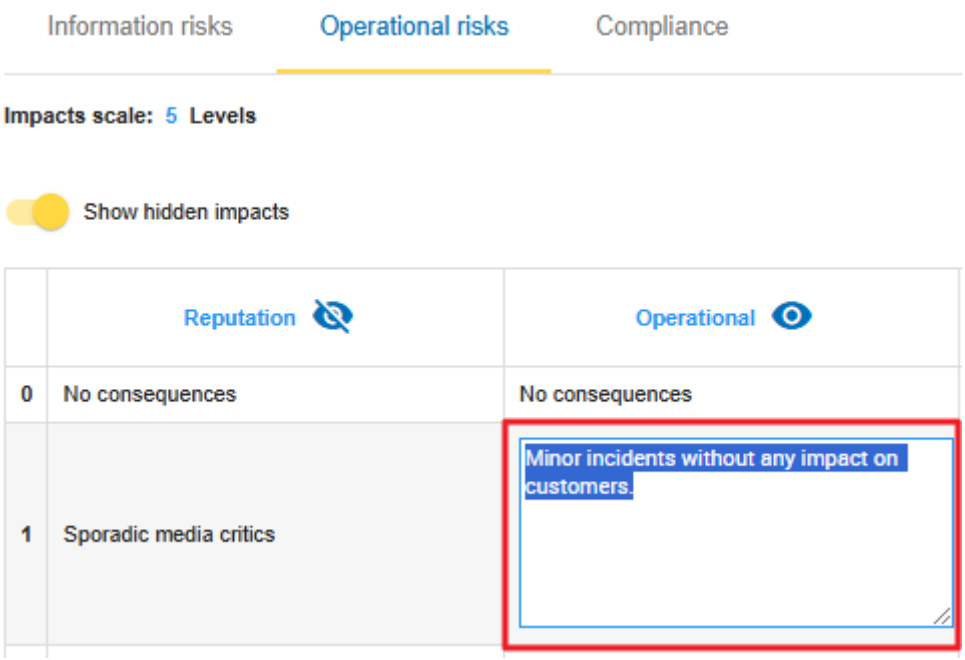
The first table is the Operational Risk Impact Scale. By default, it has 5 levels, but you may edit it by clicking on the number and provide a different value. In the below example, the Operational Risk Impact Scale has 5 levels (from zero to 4) and 5 impacts (Reputation, Operational, Legal, Financial, and Personal).



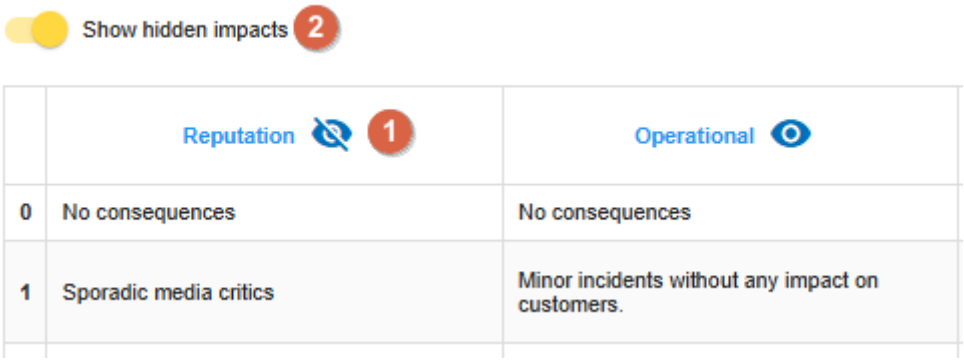
	Reputation	Operational	Legal	Financial	Personal
0	No consequences	No consequences	No consequences	No consequences	No consequences
1	Sporadic media critics	Minor incidents without any impact on customers.	Small probability of any sentences, or really slight one. Any prosecution should be futile.	Brings some marginal fees (more or less 1% of the sales revenue).	Some inconvenience which will be topped without difficulty (Time waste, procedure reiteration, irritation, etc.).
2	Temporary degradation of the company or staff reputation. Occasional media critics	Isolated incidents with a manageable impact on customers.	Possible sentence for the company.	Brings some non-marginal fees (more or less 5% of the sales revenue).	Significative inconvenience which could be topped with some difficulties (Additional costs, denial of access to commercial delivery, fear, misunderstanding, stress, slight physical ailments, etc.).
3	Strong degradation of the company or staff reputation. Serious and repeated media critics.	Interruption of a whole department.	Sentence for the company.	Brings some heavy fees which can affect the company (more or less 10% of the sales revenue).	Significative consequences which could be topped, but with some serious difficulties (funds embezzlement, bank ban, deterioration of goods, job loss.).
4	Death of someone. Definitive degradation of the company or staff reputation. Internationnal media coverage.	Complete stop of all services	Heavy sentence for the company.	Brings some deadly fees almost insurmontable (more or less 20% of the sales revenue).	Significative consequences almost irremediable, which can't be topped (financial distress, important financial debts, working impossibility, long periods psychological and physiological affection, death, etc.).

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

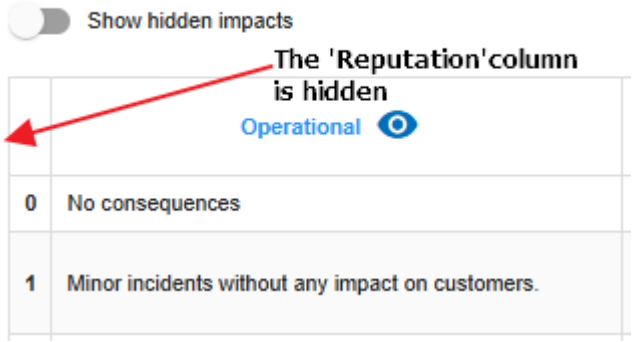
The operational risks impact scales are customisable by modifying the names of any of the existing scale names and adding custom ones. The level number can be also adjusted to the value that best fits the organisation's needs. Each of the impact levels can have a specific predefined value. The values adjustment has to be started from the bottom to extend the values definition (for example having them set in geometric progression: 0, 1, 2, 4, 8, 16...). You can edit the headings and the content of the cells by simply clicking on them, allowing you to provide different values or explanations.



You may make any impact hidden by clicking on the 'eye' icon next to the name of the impact

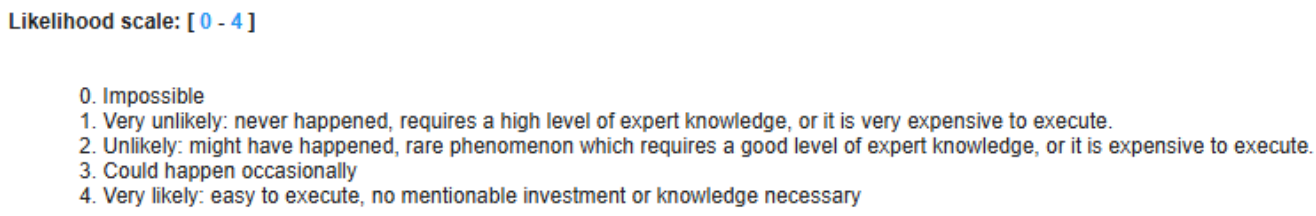


and then click on the toggle 'Show hidden impacts' to become grey:

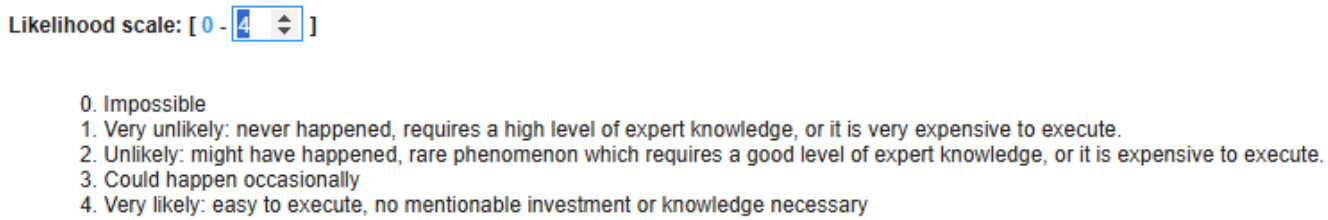


5.2.2. Likelihood scale

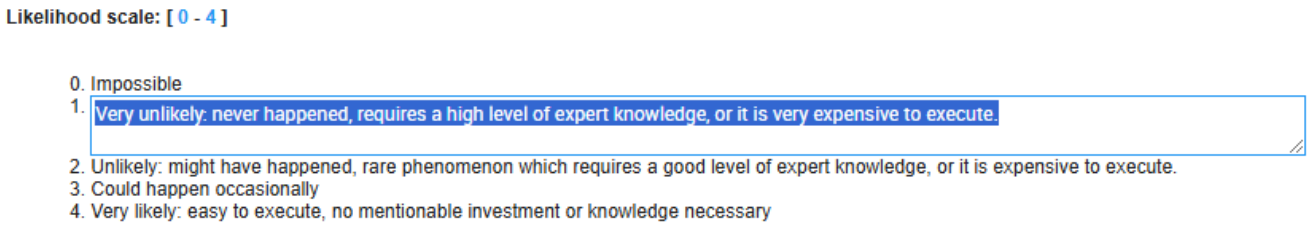
The second table is the Operational Risk Likelihood scale:



By default, it has 4 levels, but you may edit it by clicking on the number and provide a different value.

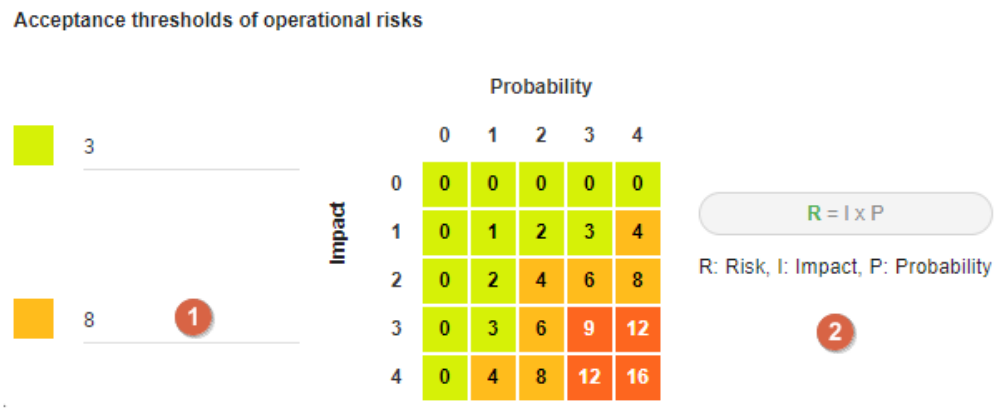


Also, you can edit the content of the cells by simply clicking on them, allowing you to provide a different explanation.



5.2.3. Acceptance threshods of operational risks

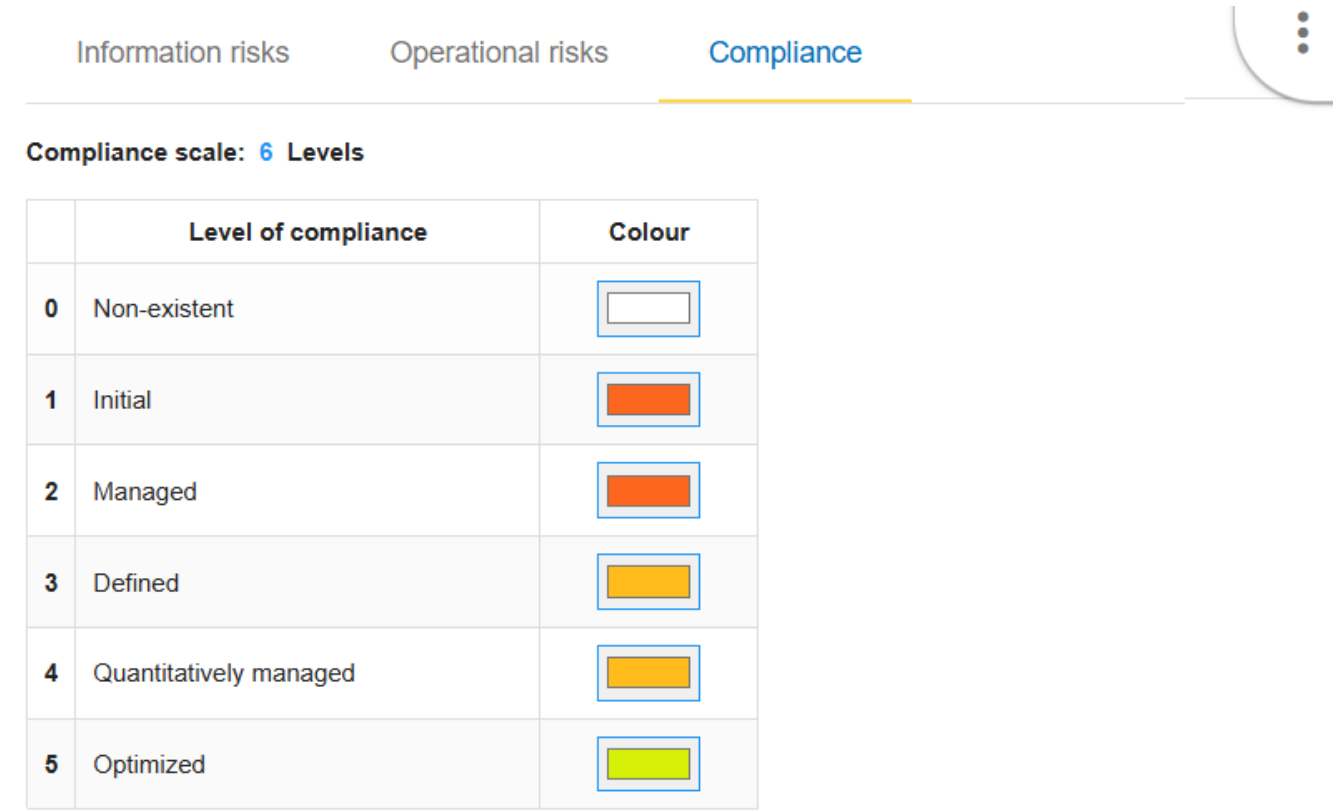
The third table is the Acceptance thresholds for operational risks.



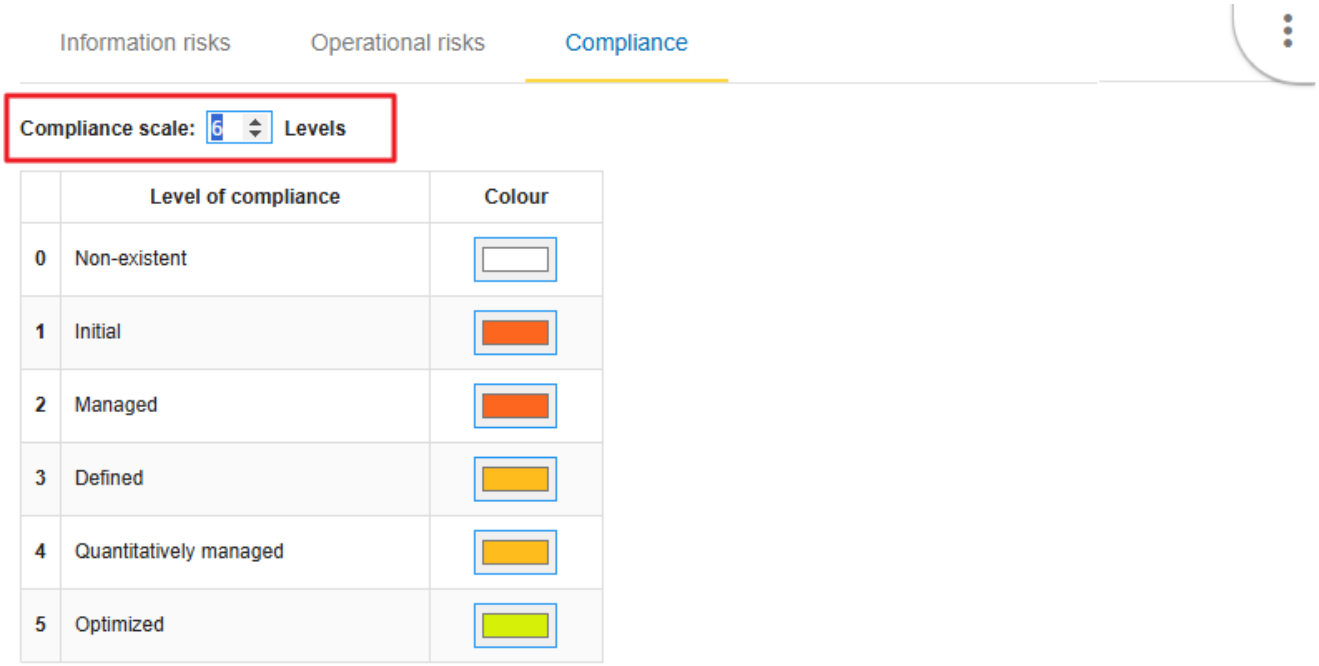
1. Modification of threshold levels of operational risks. The table displayed above (as well as the risk analysis tables) is updated automatically.
2. Operational risks are calculated using two criteria: `Impact x Probability`.

5.3. Compliance

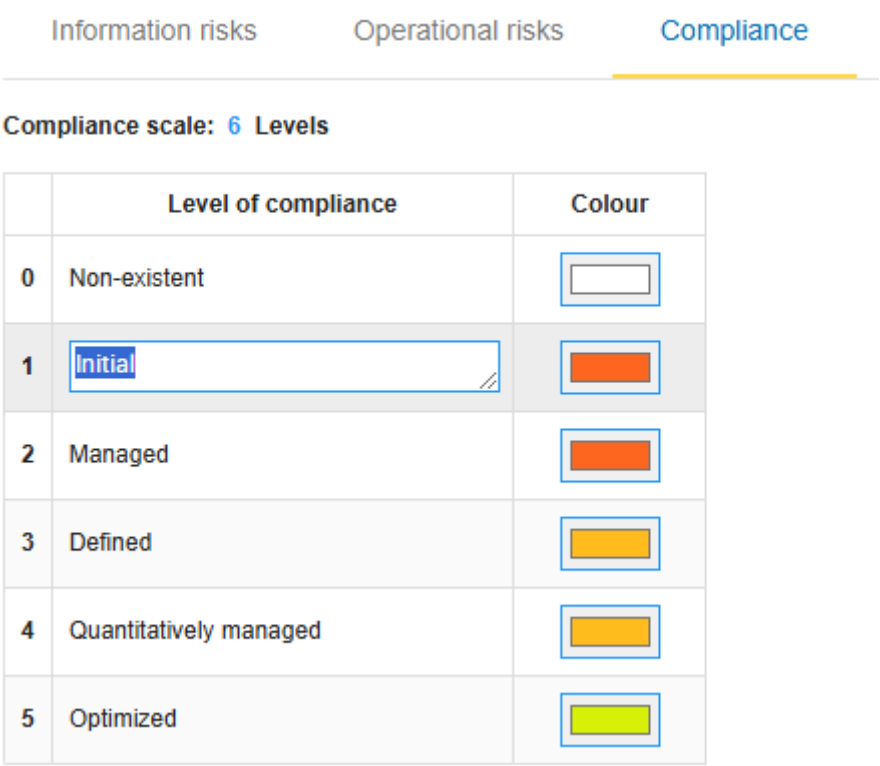
The third tab on the top of the screen is 'Compliance'.



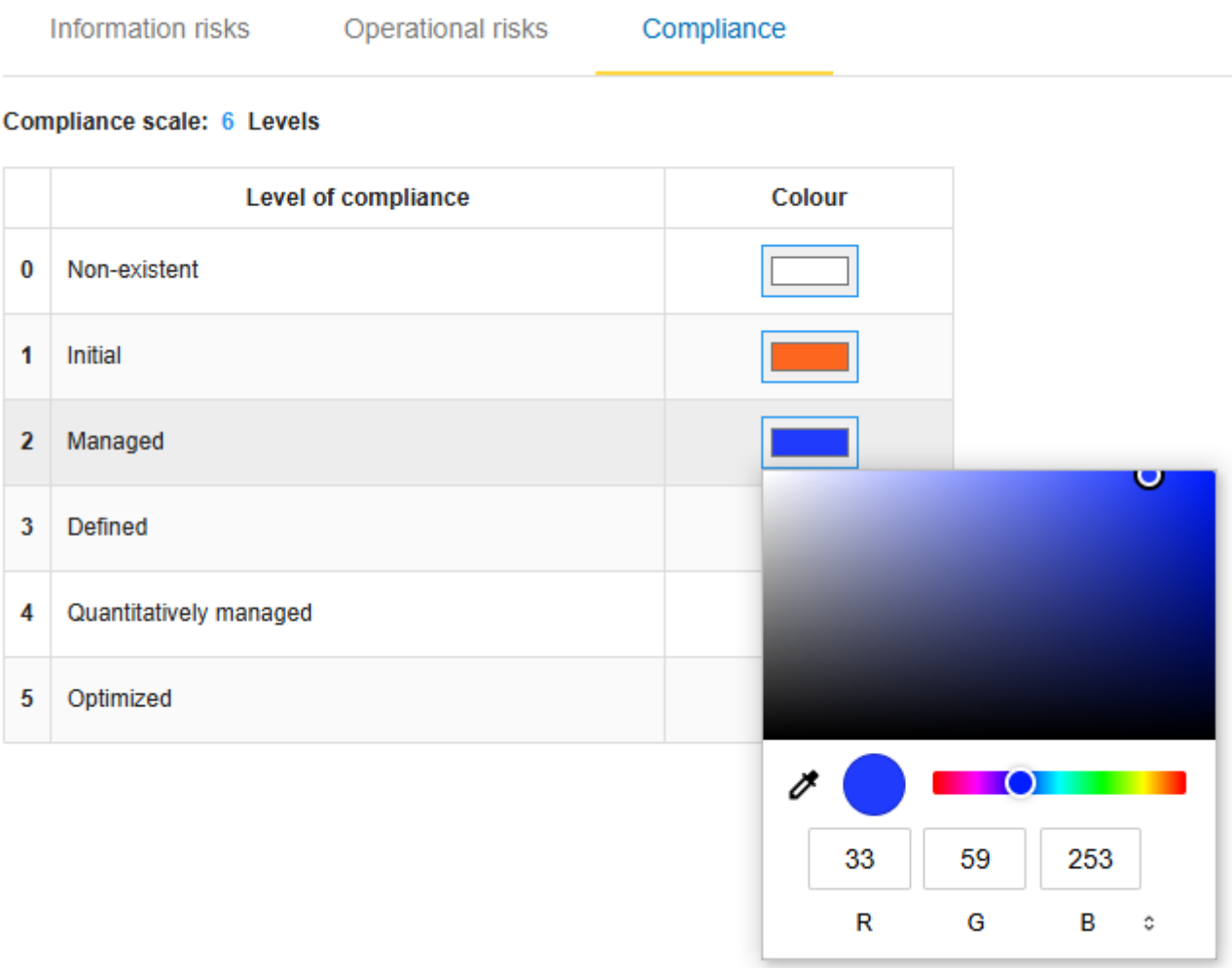
The compliance levels configuration is created to allow customisation of the “Statement of Applicability” levels and define the colours of the records highlighting when the level is selected in the table. The number of levels is customisable and the colour selection is done from the colours palette. By default, there are six levels of the Compliance scale but it can be modified simply by clicking on the level number:



All cells in the table can be modified by clicking on the given cell. You can modify the first column by changing the compliance scale level (described above). You can also edit any cells of the second column (Level of compliance):



If you want to change colour of a certain level of compliance, click on the relevant cell in the colour column. Then choose a different colour from the palette:



Since the colour for the level 'Initial' and 'Managed' were very similar (orange shade), let's change the colour for the level of 'Managed' to blue:

Information risks Operational risks Compliance

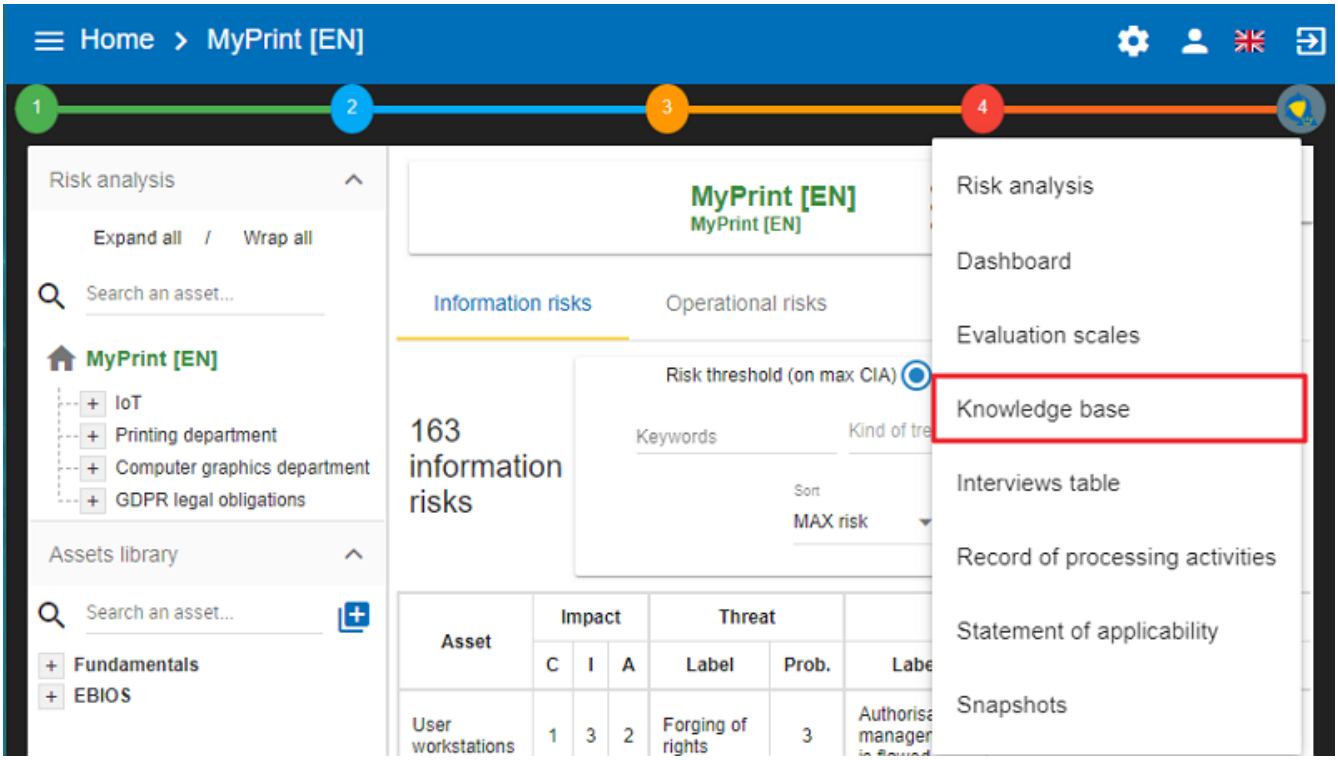
Compliance scale: 6 Levels

	Level of compliance	Colour
0	Non-existent	
1	Initial	
2	Managed	
3	Defined	
4	Quantitatively managed	
5	Optimized	

Chapter 6. Management of Knowledge Base

The knowledge base menu is always accessible from the main view of MONARC.

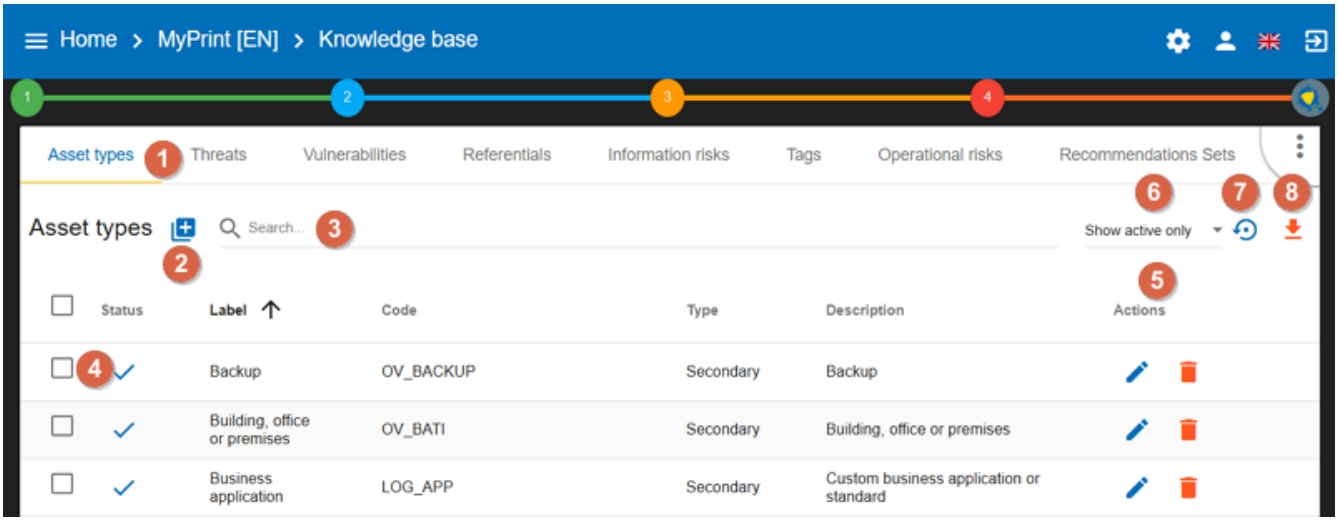
Click on the contextual menu ⋮ in the top right-hand corner of the screen and choose the submenu 'Knowledge base' from the list:



All parameters are managed with the same view. The knowledge base has the following tabs:

1. Asset types
2. Threats
3. Vulnerabilities
4. Referentials
5. Information risks
6. Tags
7. Operational risks
8. Risk Sources
9. Recommendation sets

In the User Guide, the tabs will be explained in the above order. The knowledge base opens with the 'Asset types' tab and contains the following main functionalities:

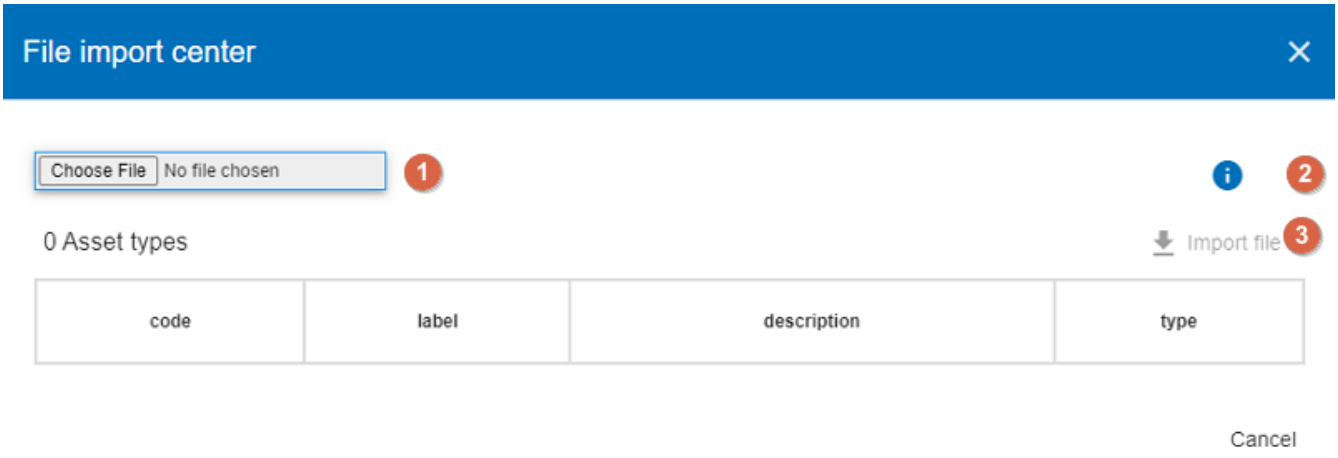


1. `Select` the desired parameter tab.
2. Add a `parameter` according to the active tab.
3. `Search for` a parameter.
4. `Select` a parameter (for manipulation).
5. `Edit/delete` selected parameters.
6. `Show active only`: by clicking on the field, you may choose 'Show inactive only' or 'Show all'.
7. `Reset filter` : You may reset the filter to the original setting by clicking on the arrow turning to the left.
8. `Export CSV`: You can export the knowledge base objects by clicking on the downward pointing orange arrow. You can export (and later import) the complete Knowledge Base objects ether with the analysis data or without. This way the Knowledge Base of the analysis can be shared.

Most parameters have a code, label, and description. `Risk Sources` are the exception: they use a label only, because the selected label is displayed directly in the risk tables, risk sheets, and exports.

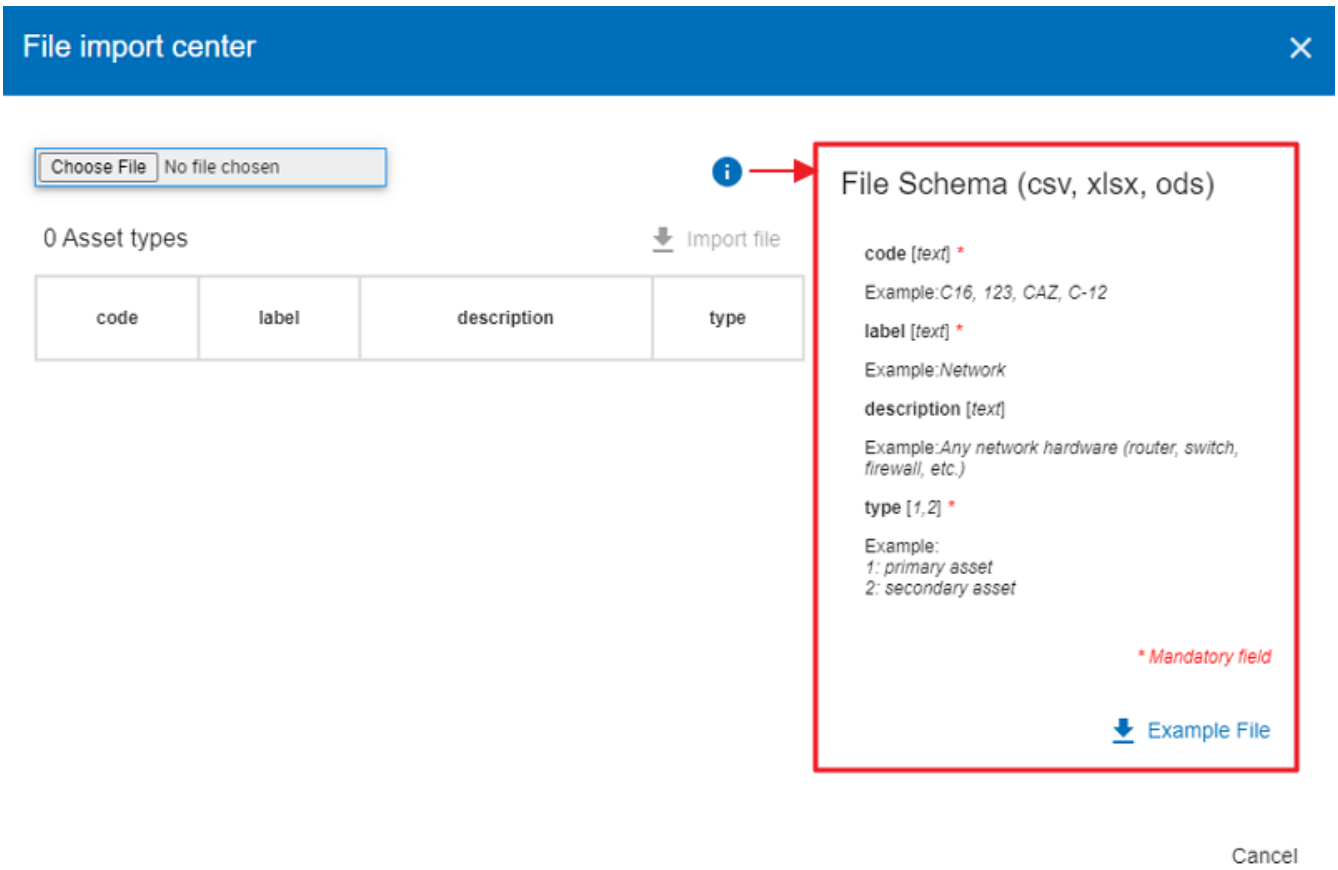
- The code is used to categorize the parameter.
- The label is displayed in all MONARC views.
- The description is the label that typically appears in the tooltip.

If you click on the ‘Add an asset’ icon, the ‘Add an asset type’ window appears. You can add assets by importing them from a file or from MOSP. If you choose to import an asset/assets from a file, the ’File import center’ appears.



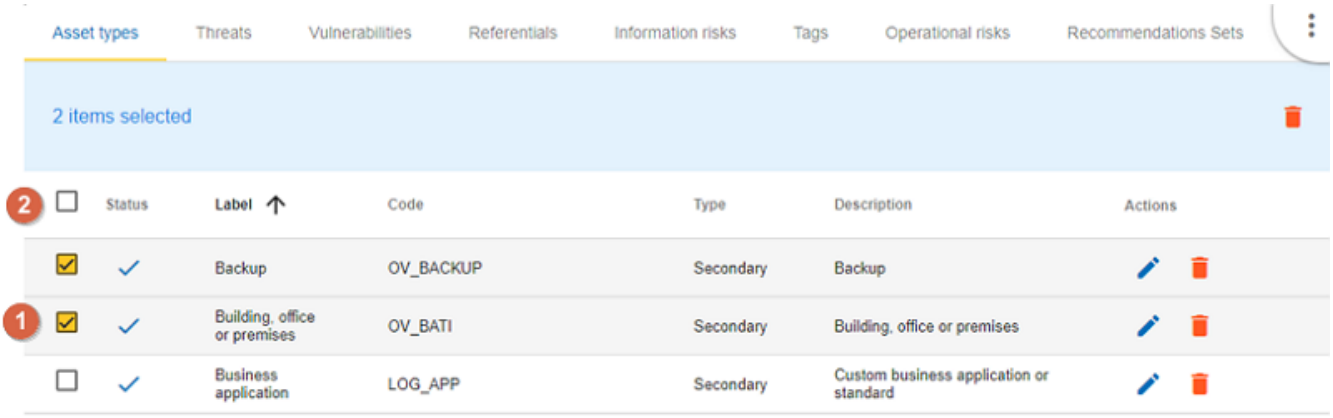
1. You can choose a file to upload it.
2. You can get information on the form and content requirements related to the file to be uploaded.
3. You can import the file.

If you click on the 'I' icon, the File Schema popup appears, which provides additional information about the mandatory fields to populate when creating a file to be uploaded.



Chapter 7. Selecting assets separately or as a group

You can select assets separately by clicking on the checkbox in front of the relevant asset (1), or you can select all the assets in the list by choosing the top checkbox next to the column header called ‘Status’ (2).



7.1. Type of assets

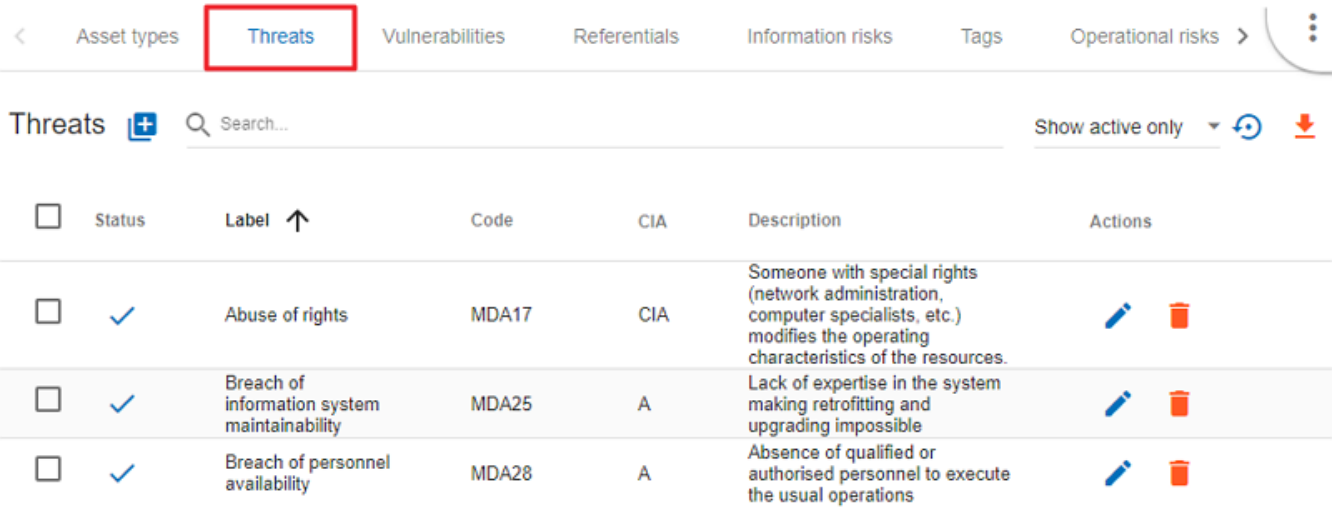
There are two types of assets:

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

7.2. Threats

The essential parameters of threat threats are in alignment with the CIA criteria. It is important when creating a new threat to properly specify these criteria, because they will influence 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.

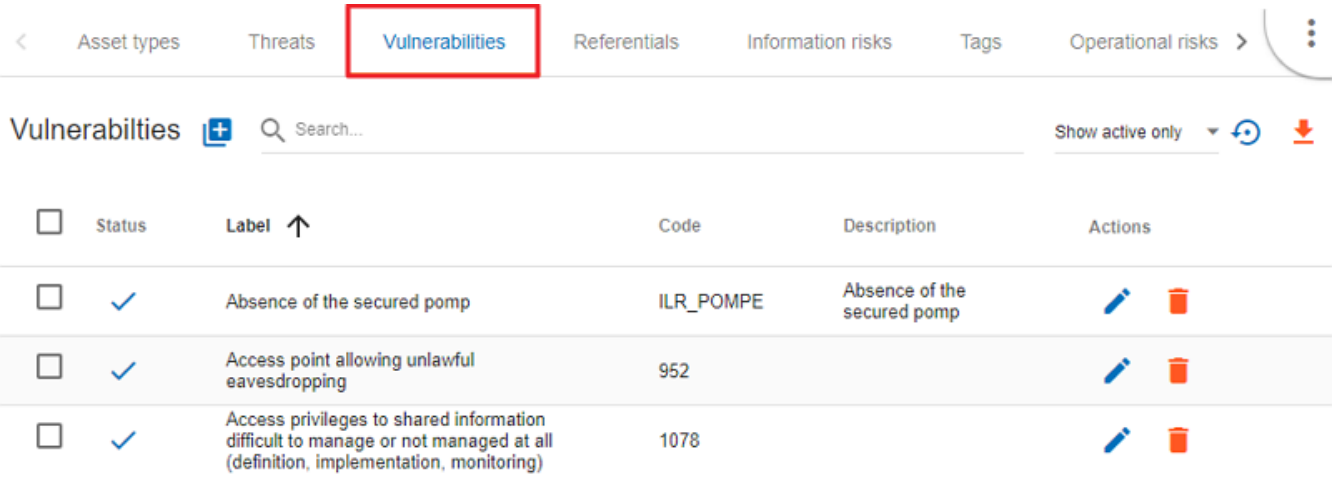
The screenshot below shows an example of what the Threats table looks like. As you can see, its structure is very similar to that of the Asset types table, and you can perform the same operations with the elements.



7.3. Vulnerabilities

Vulnerabilities must negatively describe the risk context. The greater the vulnerability, the less existing or effective the 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 refine a questionnaire or the precise points that are sought about a risk.

The screenshot below shows an example of what the Vulnerabilities table looks like. As you can see, its structure is very similar to that of the Asset types table, and you can perform the same operations with the elements.



7.4. Referentials

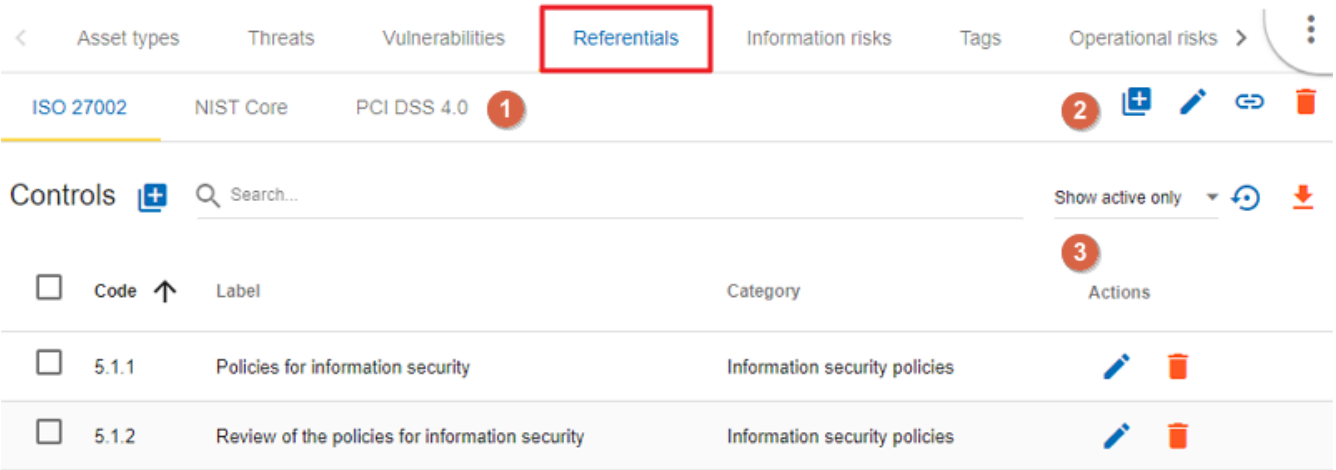
It is a repository used by default to assist in the implementation of controls for managing a specific risk.

New in MONARC v2.14.1: CyFun referentials

From MONARC v2.14.1, the 2025 `CyFun Basic`, `CyFun Important`, and `CyFun Essential` referentials are available by default in the referential list when creating a risk analysis. Select one or more of them as linked referentials, then manage their controls from this `Referentials` tab and use them in the Statement of Applicability.

The CyFun referentials can also be imported from the MONARC Objects Sharing Platform (MOSP). In the `Referentials` tab, select `Add`, then `Import from MOSP`, and search for `CyFun` to select the required referential.

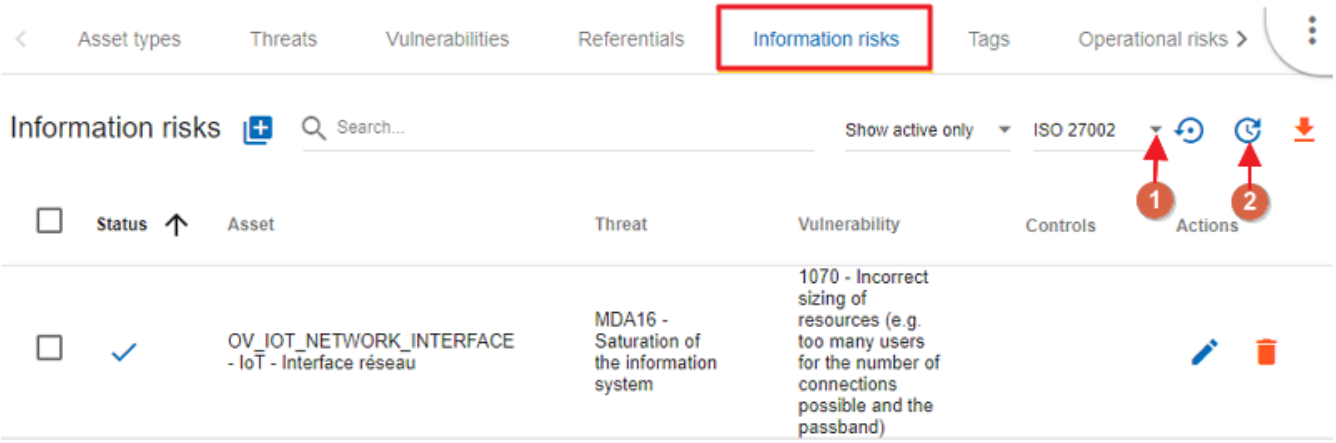
The CyFun referentials include mappings to ISO 27002 controls. When both referentials are linked to an analysis, use the existing referential matching and control-update functions to work with these mappings. See issue #616 for the associated release item.



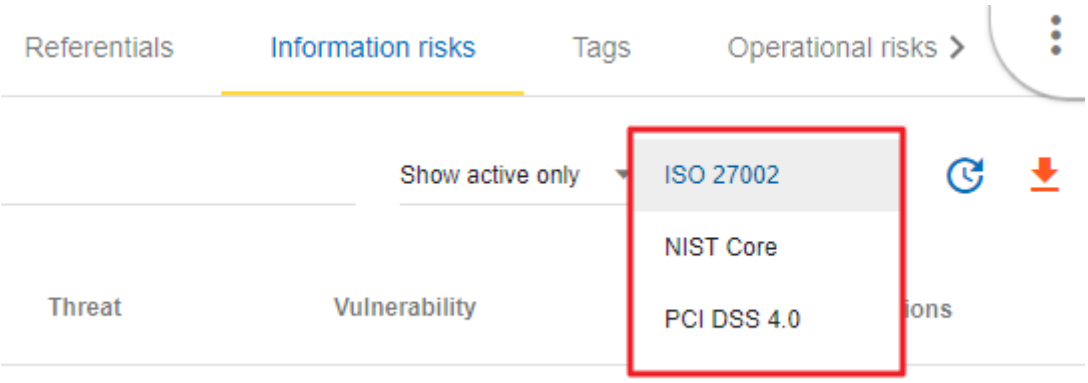
1. This area is dedicated to managing the selection of referential. On the right, there are the standard buttons to edit, add, and delete a referential.
2. This new icon appears when you have two referentials. It allows you to add, import or export matching between the selected referential and the others.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

7.5. Information Risks

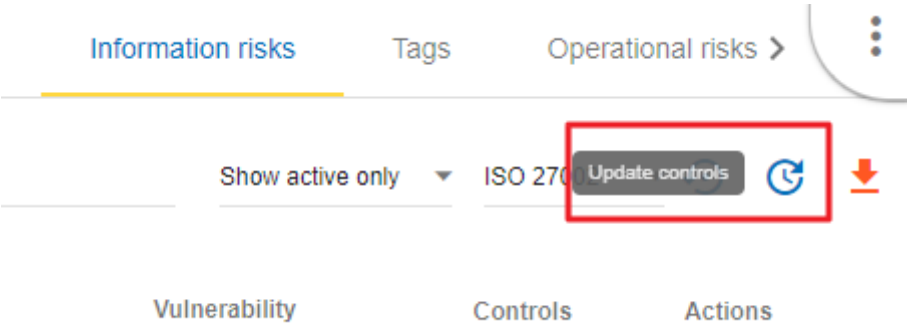
This table is the core of MONARC's knowledge base. This is where associations between 'Asset Type,' 'Threat,' and 'Vulnerability' are made. The combination of risks inherent to each asset will be proposed by default when the risk model is created. For each association, which can be considered a risk scenario, it is possible to link security measures from the referentials tabs. Only supporting assets are available for Threat/Vulnerability associations.



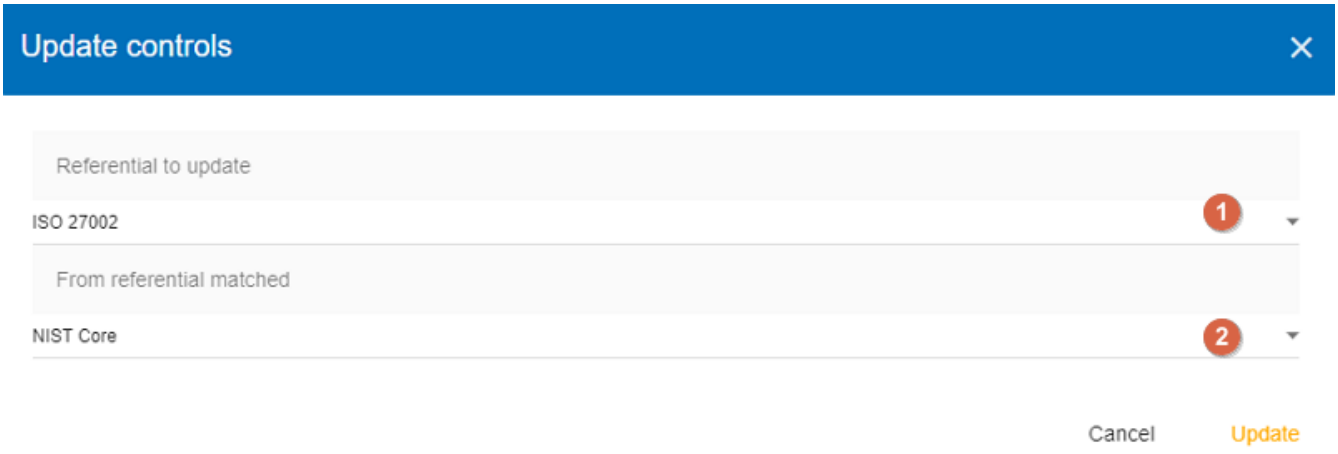
It is possible to switch between referentials to see their linked controls of the risks shown below. Use the down-pointing arrow, so you can choose between the options that appear.



This new icon (Update controls) appears when you have two referentials. It allows you to automatically linked controls of a referential to risks. It uses the matching defined in the step before.



The Update controls popup opens, where you can use two drop-down menus to match two referentials.

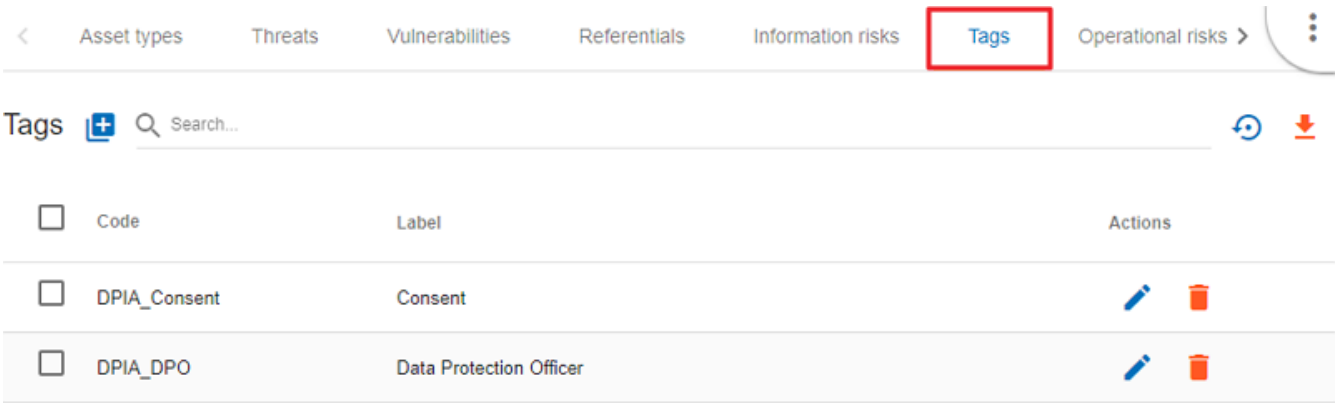


1. The first referential is the one which you want to link to the risks.
2. The second is the source you want to use (it has taken risks linked to its controls).

7.6. Tags (Operational Risks)

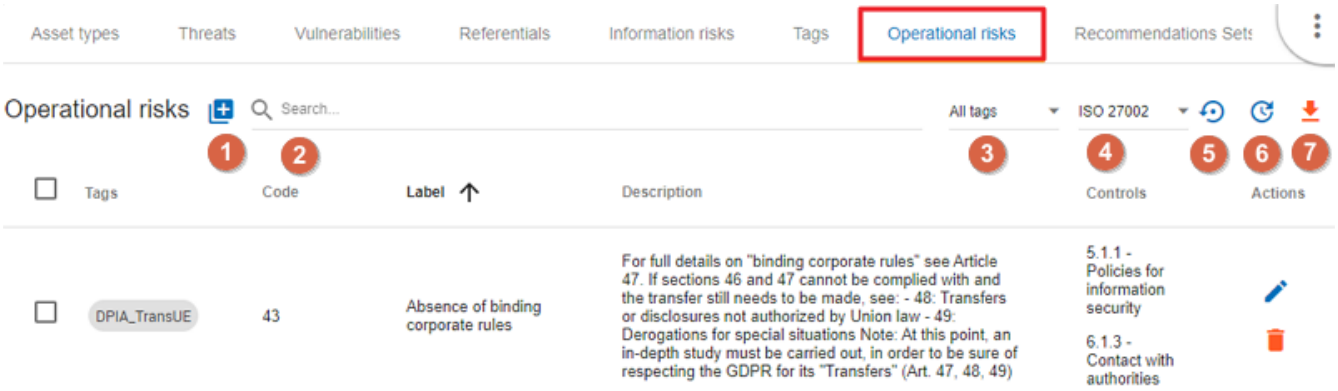
The layout of the Tags table is very similar to the previous ones. Just like with the tables described above, you can add an element (tags), search among elements, reset the filters, or export the items as a CSV file.

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



7.7. 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 to the risks of the information.



1. Add an operational risk
2. Search among operational risks
3. Filter among tags
4. Choose between standards (ISO 27002, NIST Core, etc.)
5. Reset filters
6. Update controls
7. Export into a CSV file

7.8. Risk Sources

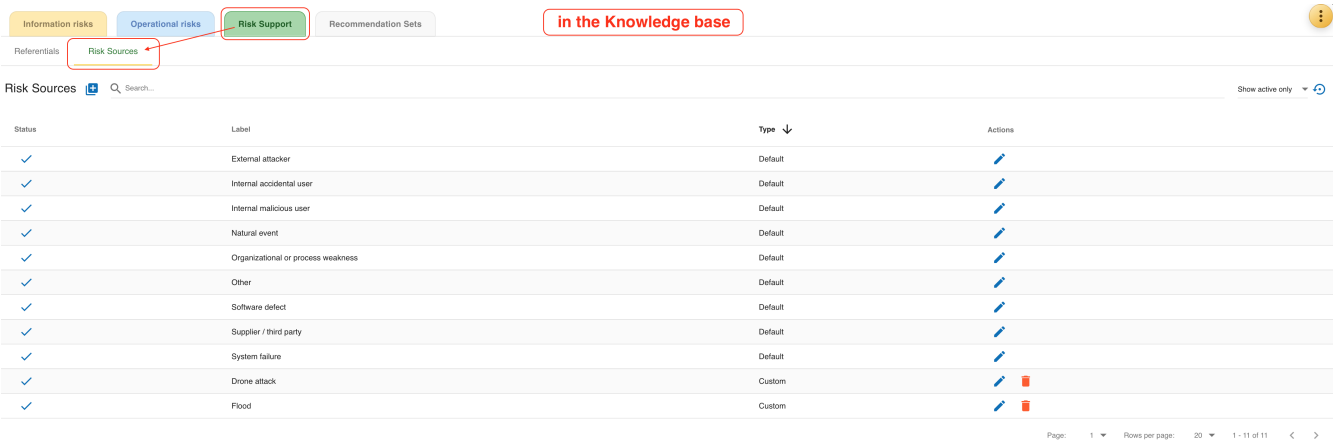
ISO 27005:2022 adaptation

The `Risk Sources` tab introduces a reusable catalog of actors, origins, or causes that can be assigned to information and operational risks. It is the central place for maintaining the labels later shown in risk tables, risk sheets, and reports.

The `Risk Sources` tab lets you:

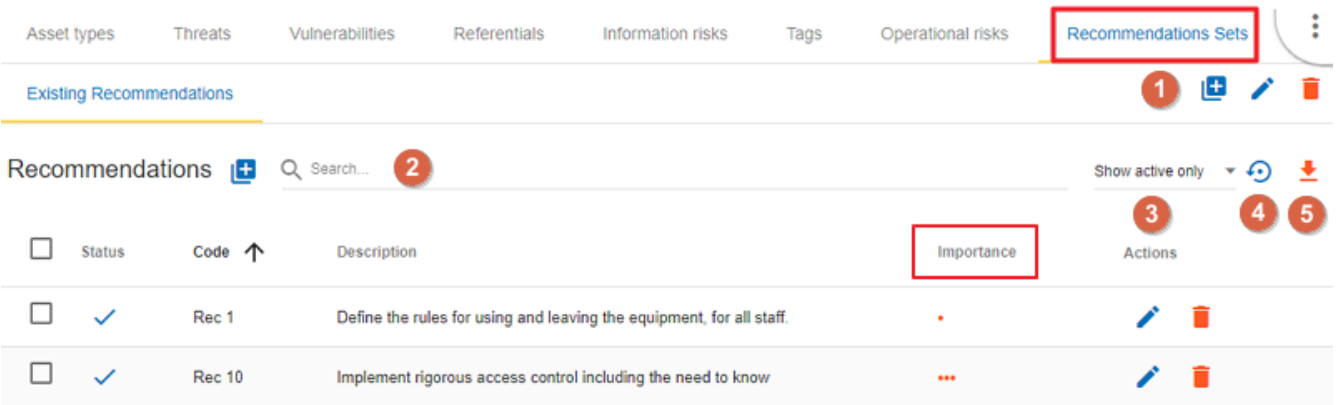
1. Add a new risk source.
2. Search existing sources by label.
3. Filter the list by status (`Show all`, `Show inactive only`, `Show active only`).
4. Activate or deactivate a source through the `Status` column.
5. Edit an existing source label.
6. Delete a custom source when it is no longer needed.

The table contains the columns `Status`, `Label`, and `Type`. The `Type` value distinguishes the default MONARC entries from custom sources created by the analyst. New sources created here become directly available in the information and operational risk sheets of the same analysis.



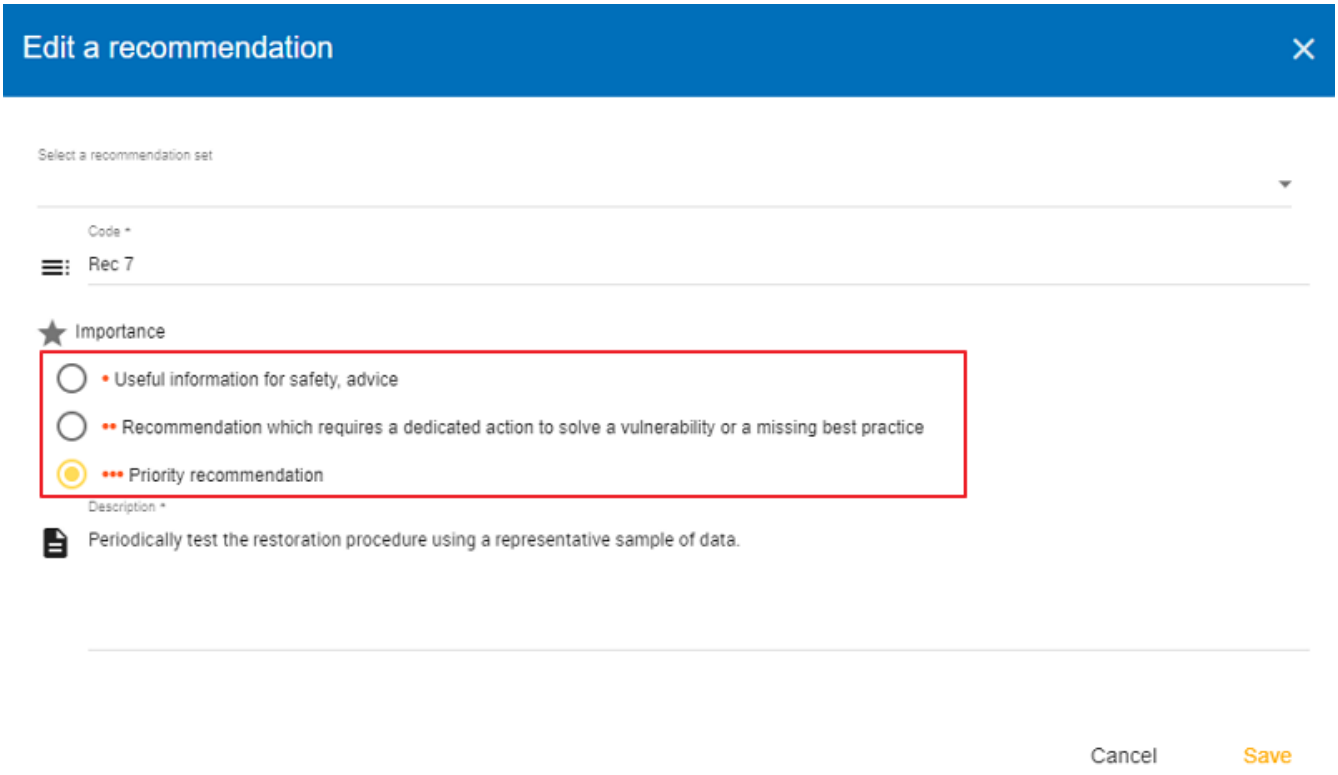
7.9. Recommendations Sets

The Recommendations Sets table is the repository that is used by default to manage the recommendations.



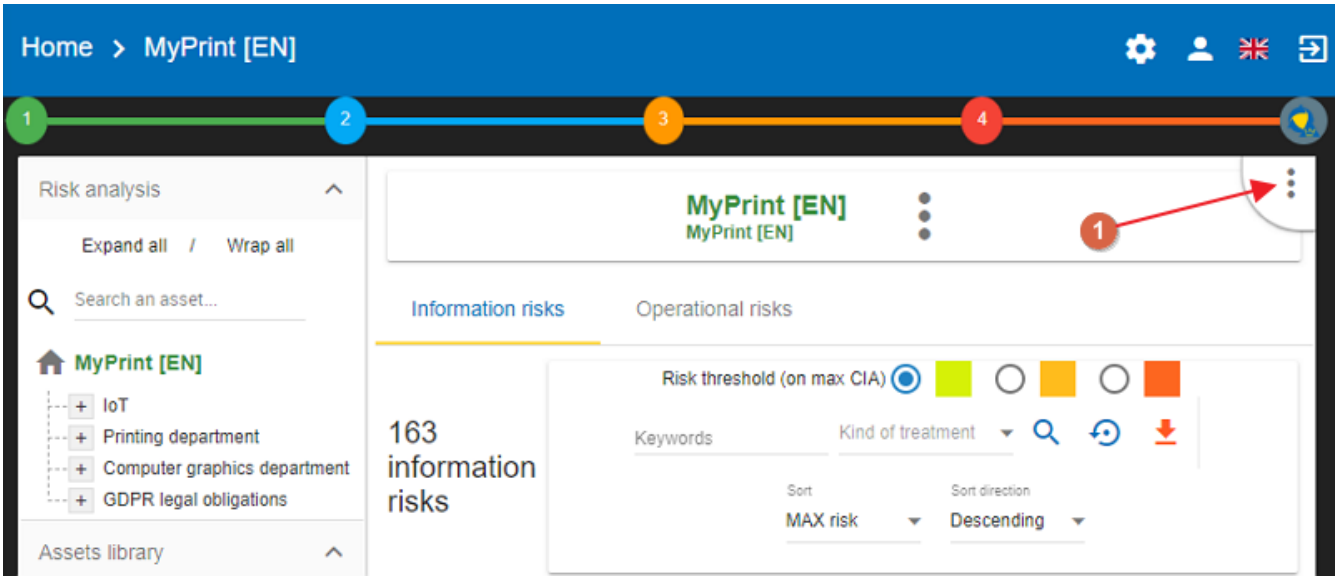
1. Add, edit, or delete a recommendation
2. Search among the recommendations
3. A drop-down menu to choose from to ‘Show all, only the inactive, or only the active recommendations
4. Reset filters
5. Export recommendations as a CSV file

When you click on the pencil icon, the ‘Edit a recommendation’ window pops up. There, you can check the meaning of the column ‘Importance’.

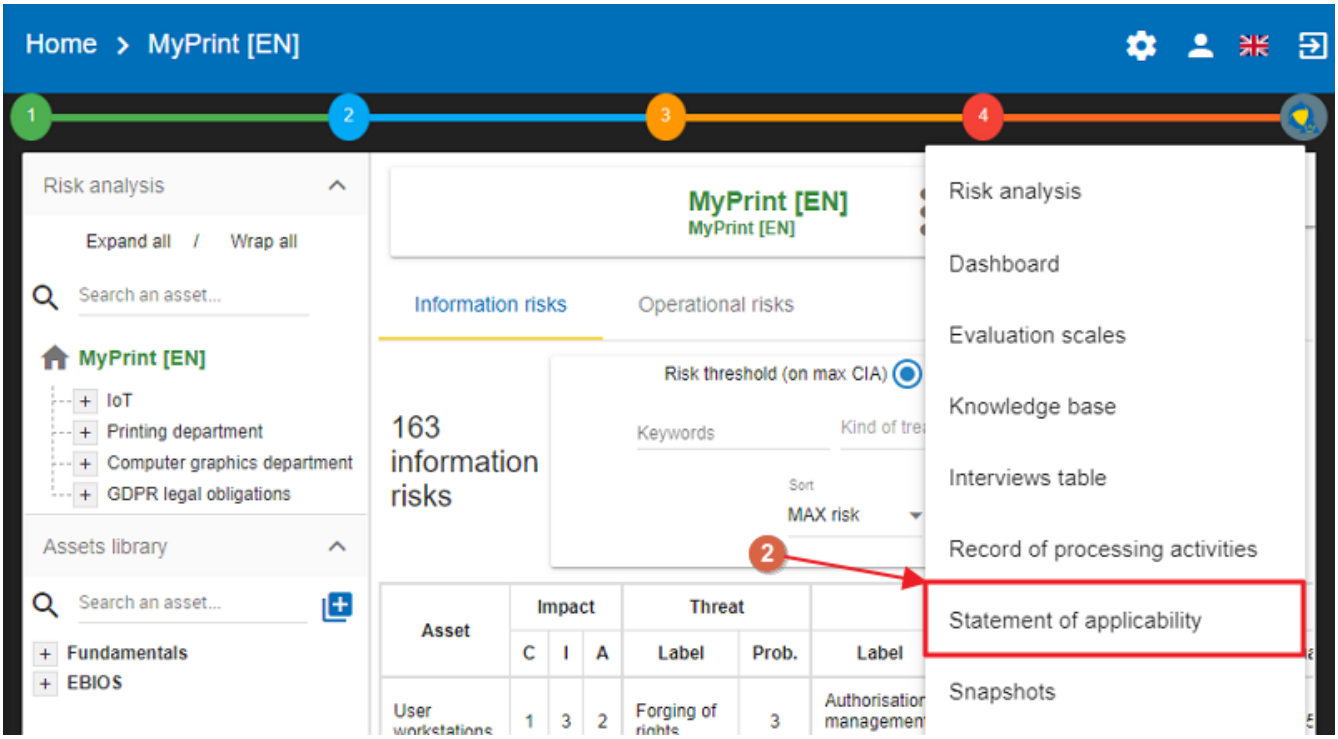

Edit a recommendation
Select a recommendation set
Code *
Rec 7
Importance
• Useful information for safety, advice
•• Recommendation which requires a dedicated action to solve a vulnerability or a missing best practice
••• Priority recommendation
Description *
Periodically test the restoration procedure using a representative sample of data.
Cancel
Save

Chapter 8. Statement of applicability

To reach the Statement of applicability screen, please click on the contextual menu ⋮ on the right:



Then, from the drop-down menu, choose the `Statement of applicability` menu item:



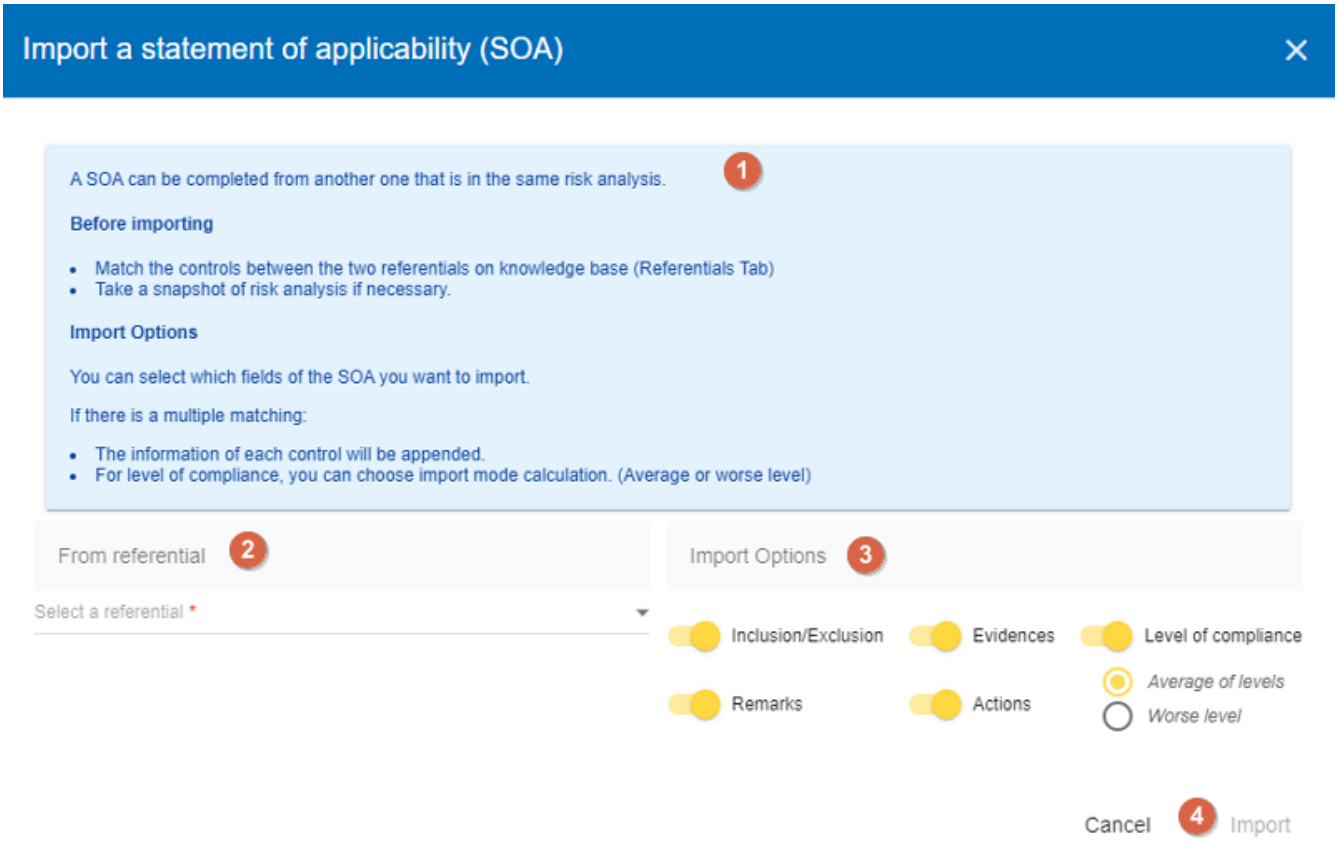
The `Statement of applicabality` screen appears:

1. Choose the `referential` (ISO 27002, NIST Core, PCI DSS 4.0) 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. To choose whether the security control is included or excluded, simply click on the acronym. A description will appear when you hover over it with the cursor.
4. The field `remarks/justification`, `Evidences`, `Actions` are text fields, just click on them and fill in the relevant cell.
5. `Export` the selected view in CSV.
6. `Import` information for the selected referential from another.
7. The Level of compliance is a drop-down list.

The inclusion/exclusion acronyms are as follows:

EX - Excluded CO - Contractual obligations BP - Best practices LR - Legal requirements BR - Business requirements RRA - Results of risk assessment

If you click on the 'Import from other referential', the Import a statement of applicability (SOA) screen appears:

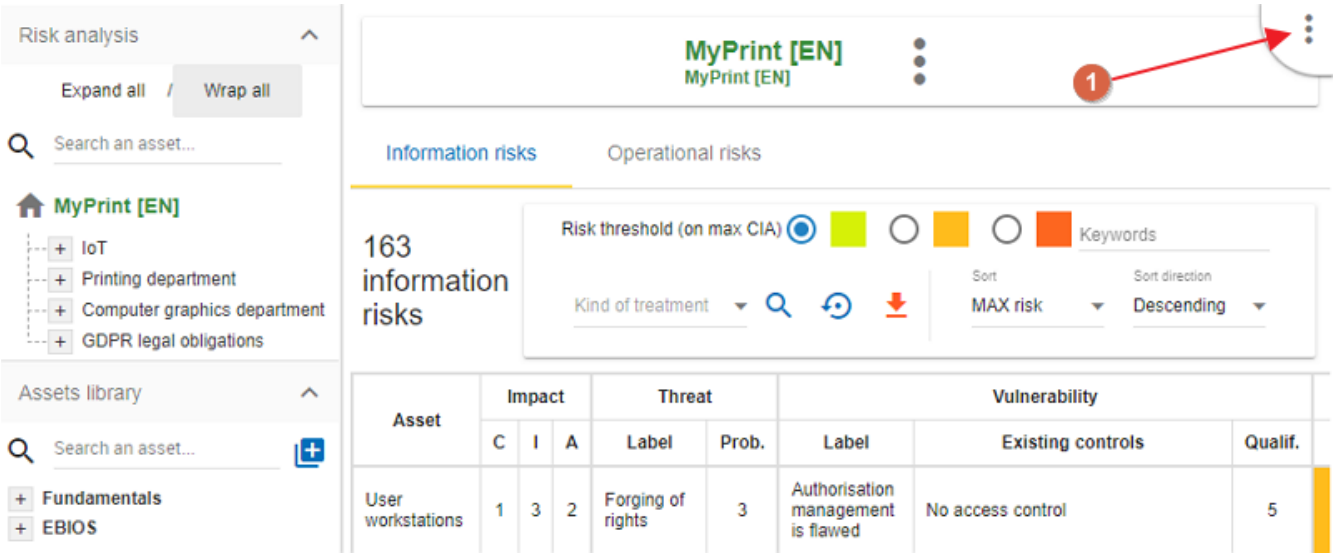


1. Please `Read` the text before importing
2. Choose the `referential` which contains information that you want to convert into the selected one.
3. Choose import options
4. Clik on the `Import` button so the information of the referential is imported.

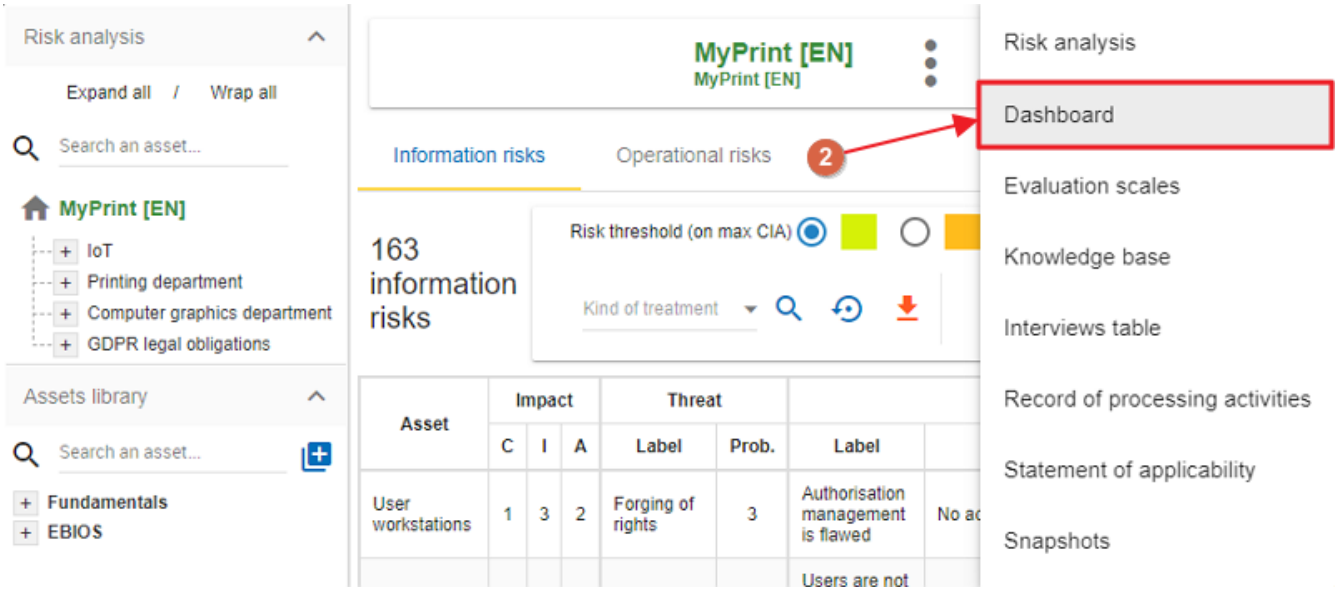
Chapter 9. Dashboard

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

1. To reach the Dashboard, first, click on the contextual menu ⋮ in the upper right-hand corner.



1. Then, from the drop-down menu, choose `Dashboard`.



The view `Dashboard` shows information about the following topics:

- Risks
- Threats
- Vulnerabilities
- Cartography
- Compliance

> Most of the charts have parameters and are exportable.

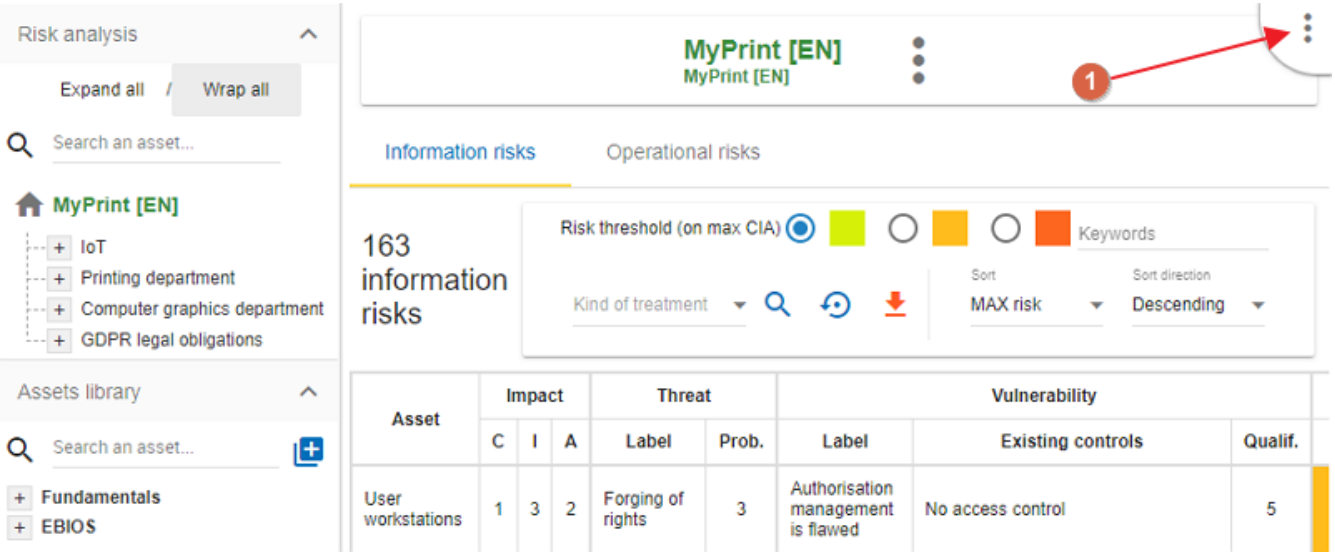
All the part of the dashboard have the same functionalities.

1. `Choose` the part on which a 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

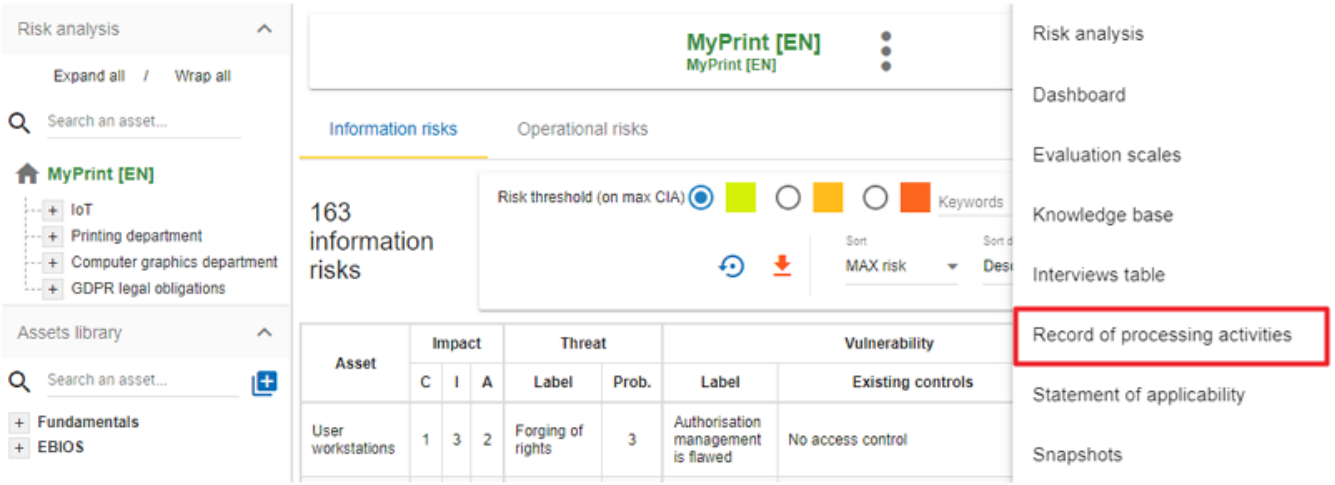
Chapter 10. Record of processing activities

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

1. To reach the 'Record of processing activities' menu, first, click on the contextual menu ⋮ in the upper right-hand corner.



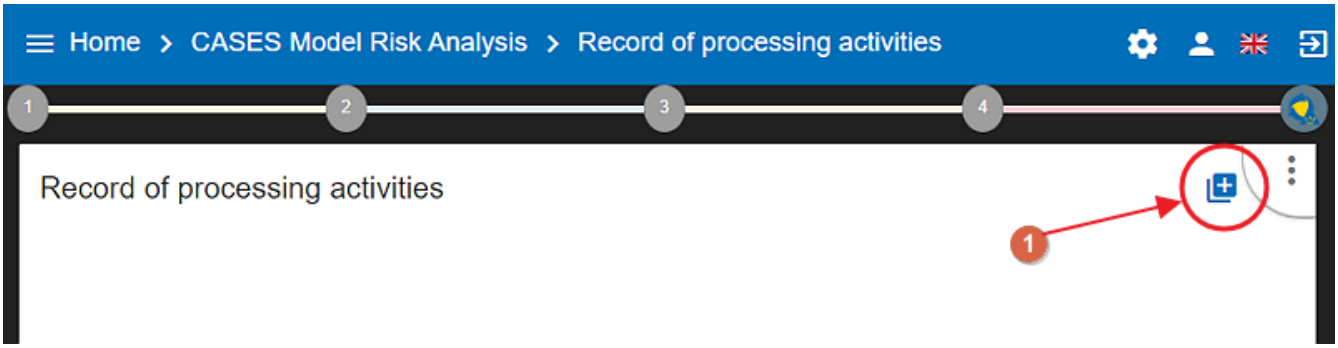
2. Then, from the dropdown-menu choose `Record of processing activites`



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

Chapter 11. How to record a processing activity?

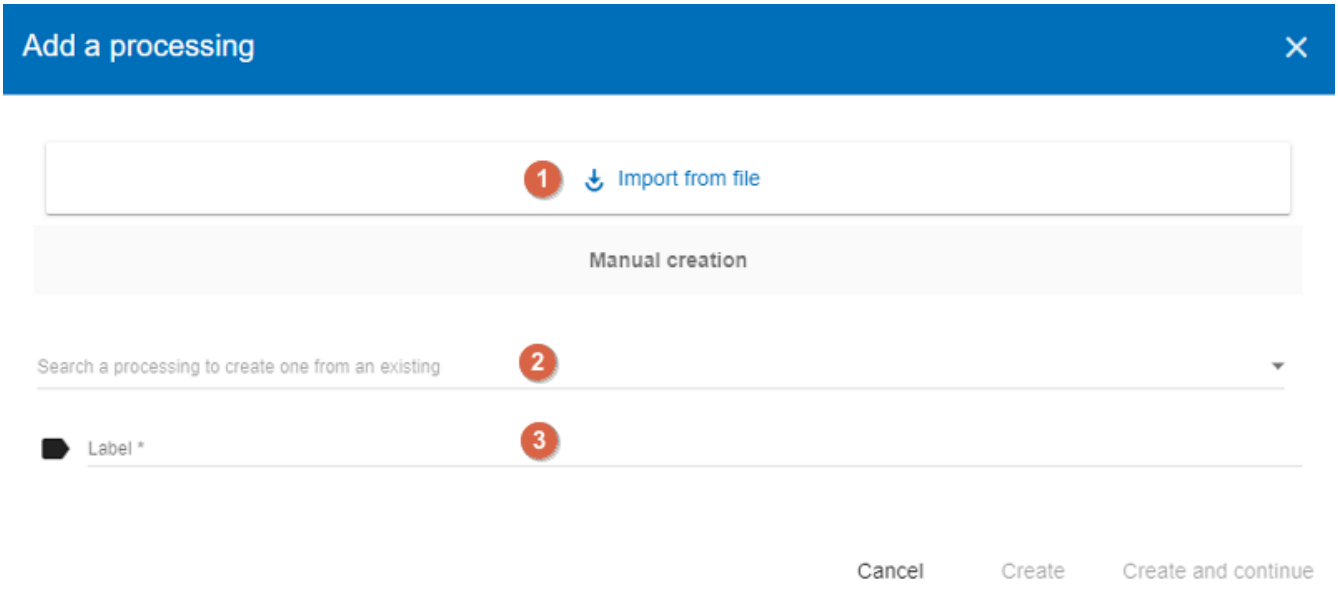
To create a processing activity, click on the + sign in the top right-hand corner of the screen:



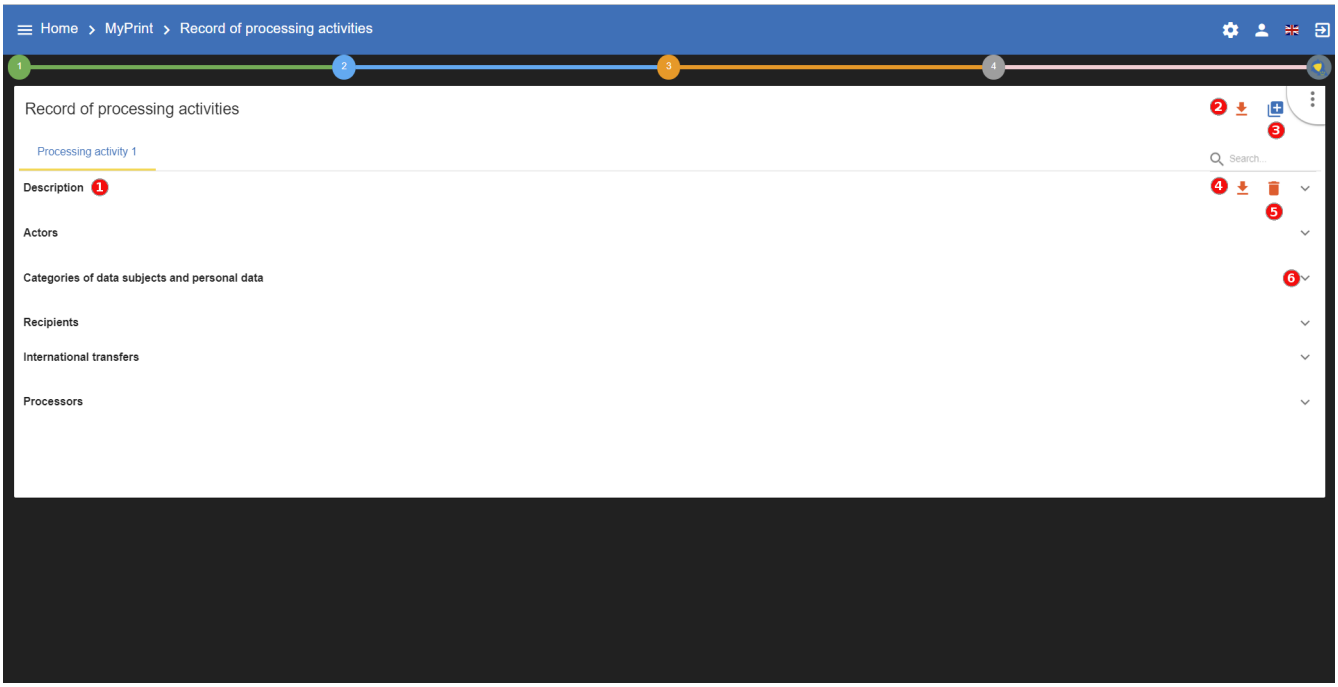
You can create a new processing activity by:

1. `Importing` a JSON file previously exported from MONARC
2. or `Creating` it from an existing one

If you create a processing activity without importing it, you have to set a label.



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



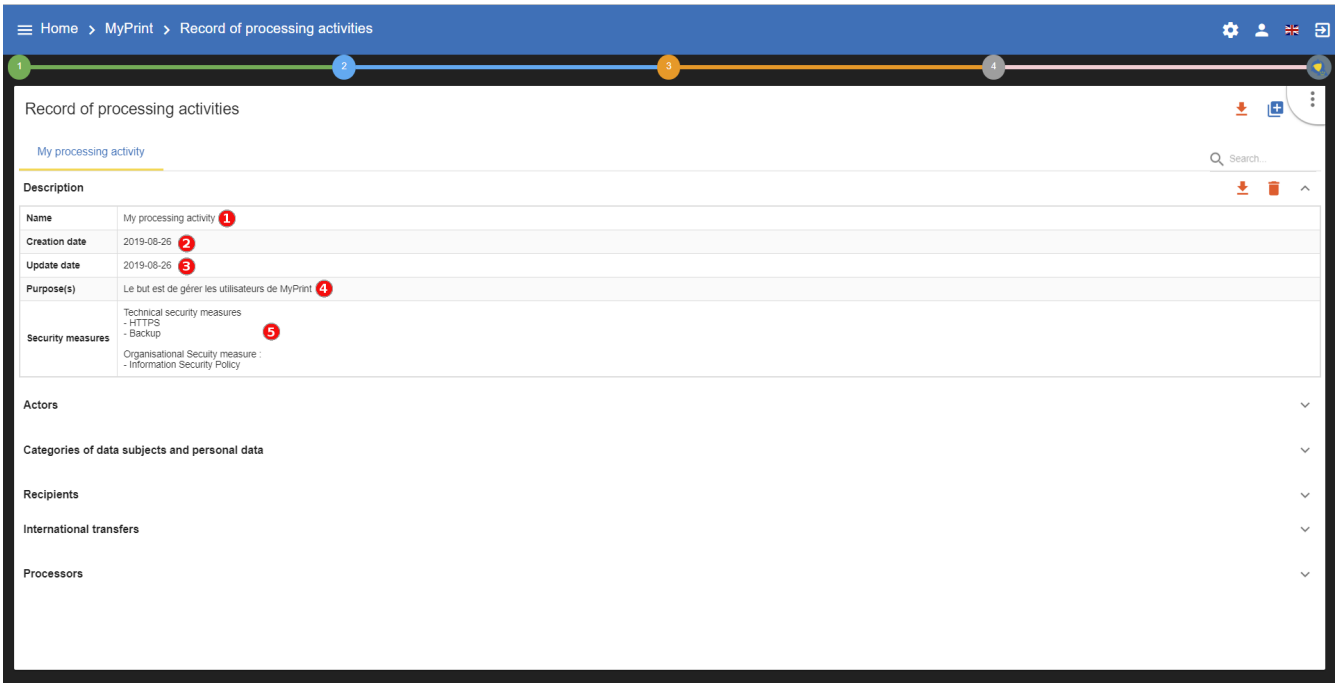
1. Fill six categories (Description, Actors, Categories of data subjects and personal data, Recipients, International transfers, Processors)

You can also :

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

11.1. Description

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

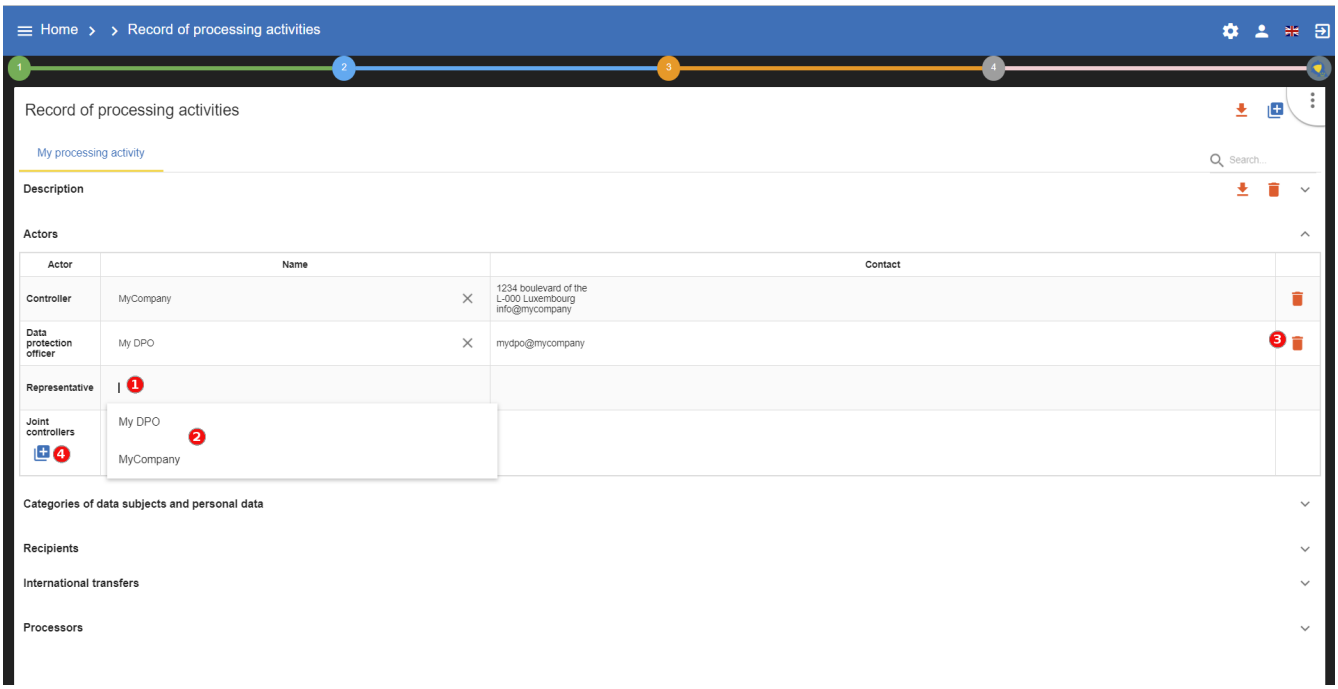


1. `Edit` the name of the selected processecing activity.
2. See the date of creation (automaticly filled by MONARC).
3. See the date of last update (automaticly filled by MONARC).
4. `Fill` the purpose of the processecing activity.
5. `Describe` the main security measures.

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

11.2. Actors

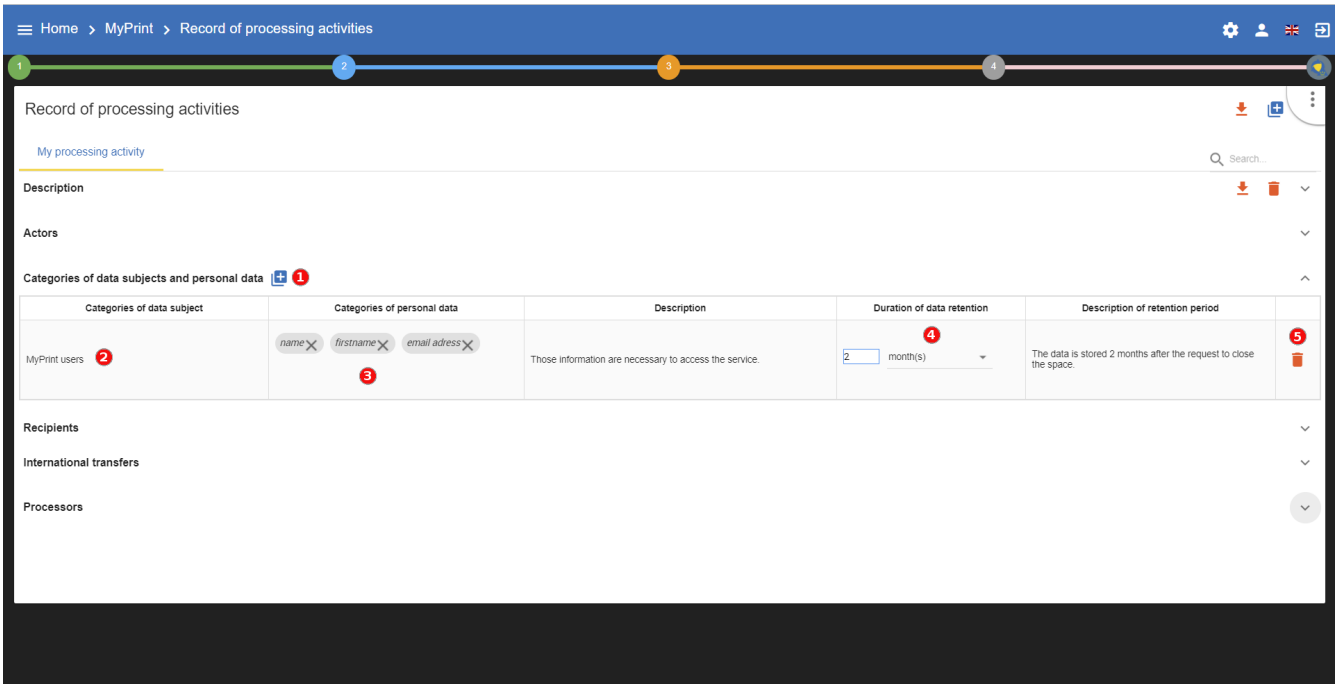
In this section you have the actors about the selected processing activity:



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.

11.3. Categories of data subjects and personal data

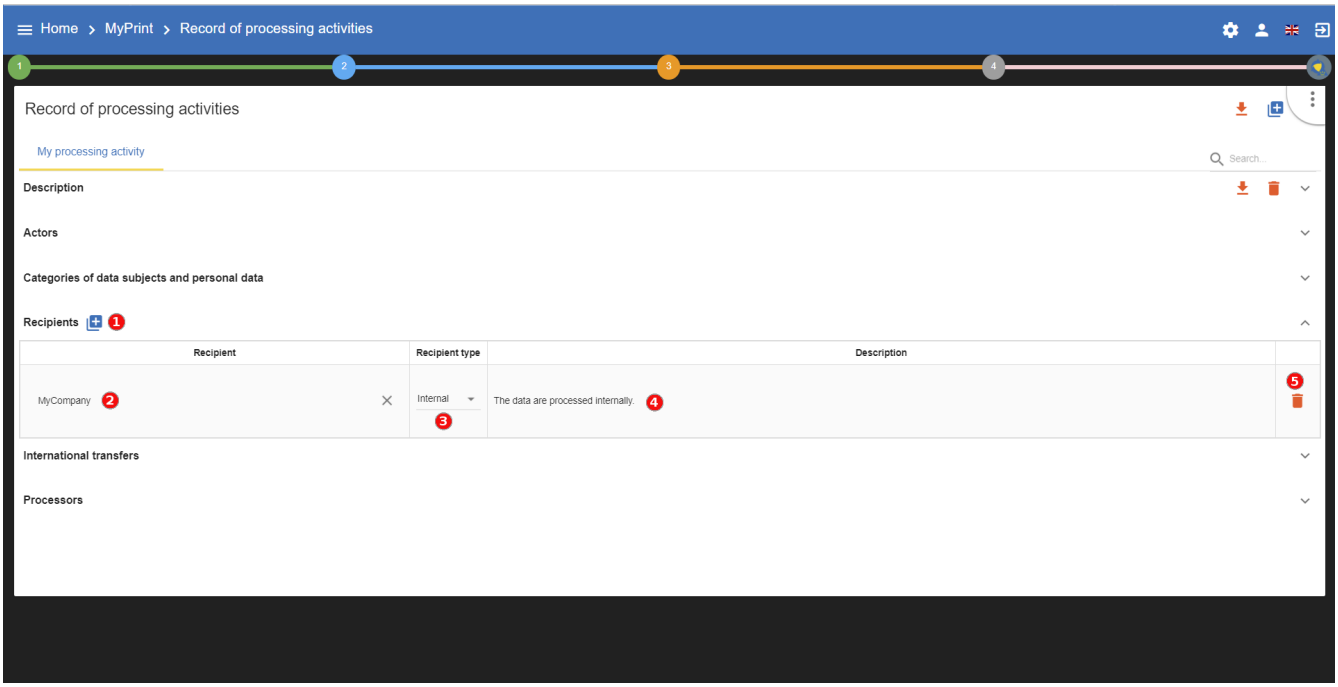
In this section you have the actors about the selected processing activity:



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.

11.4. Recipients

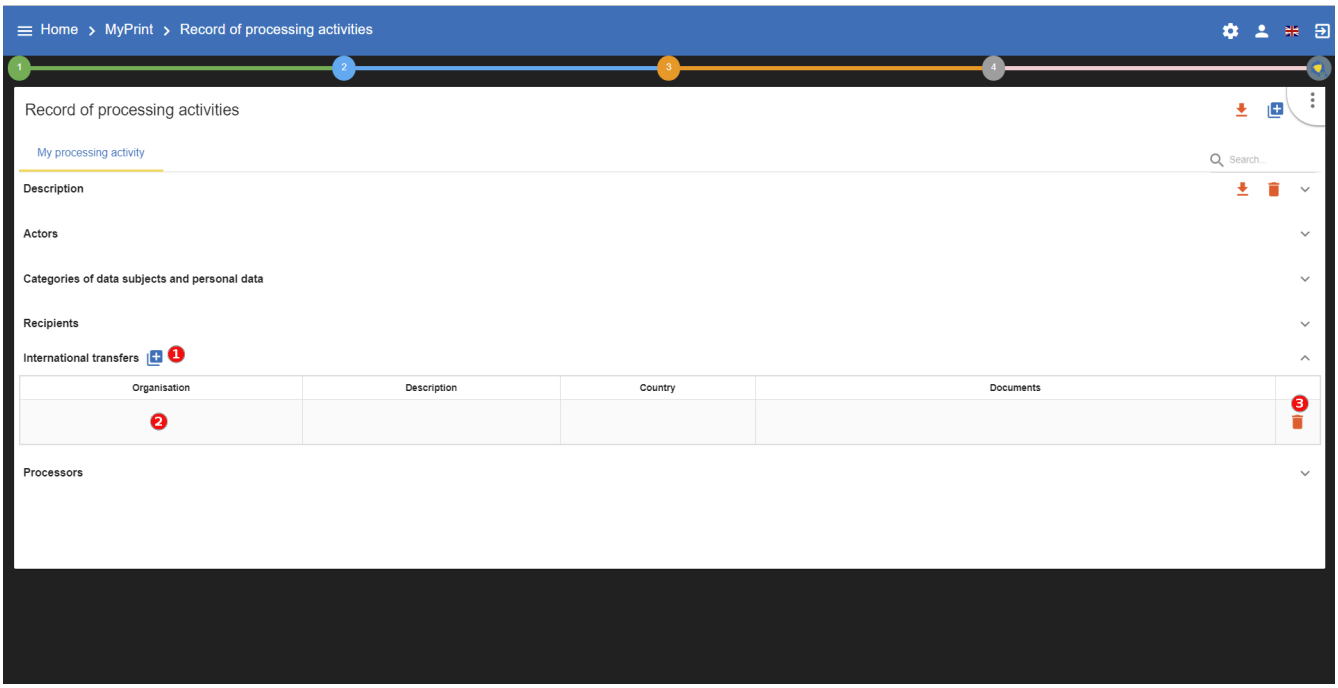
In this section you have the recipients about the selected processing activity:



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.

11.5. International transfers

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

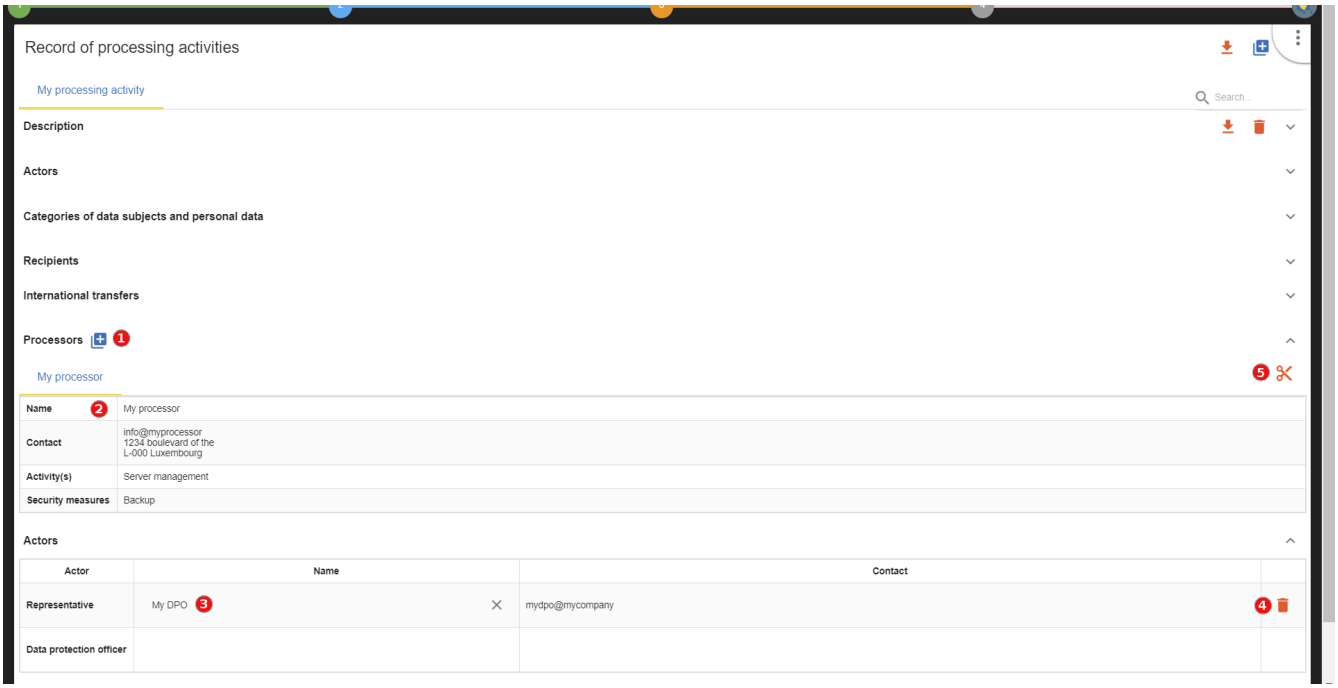


1. Add one more international transfer.
2. Organisation , description, country and documents are standard editable field.

3. `Delete` the corresponding international transfer.

11.6. Processors

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



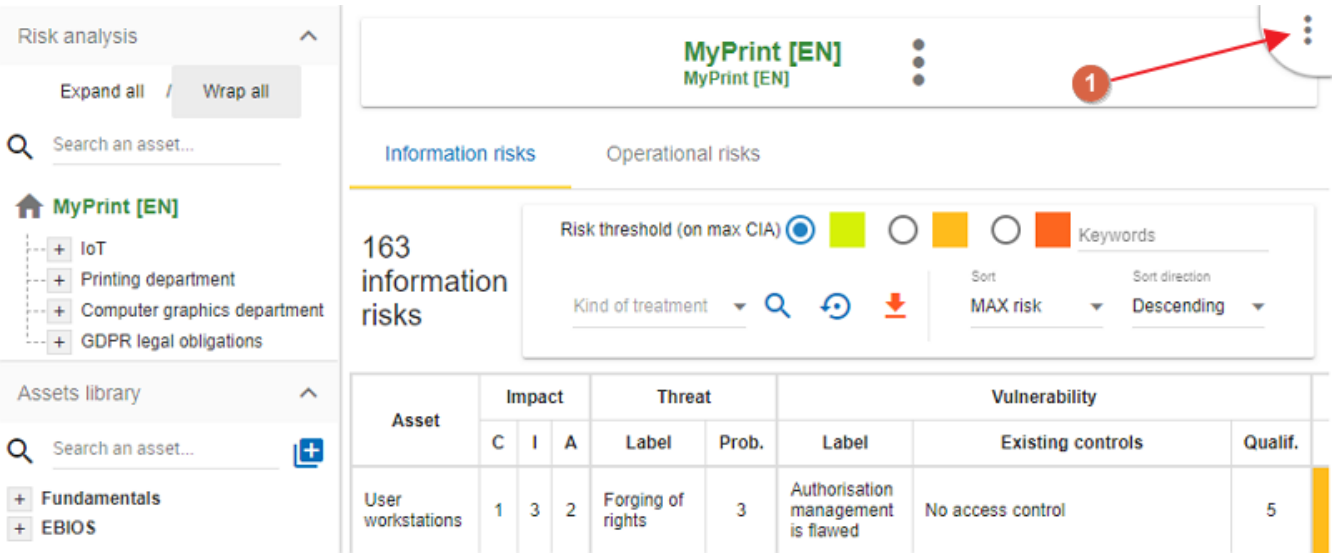
1. `Add` one more processor and feel free to select an existing one or create a new one.
2. `Name` , `Contact`, `Activity` and `security measures` are standard editable field.
3. Use an `actor` from the drop-down list or create a new one.
4. `Delete` the corresponding actor.
5. `Detach` the processor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

Chapter 12. Interviews

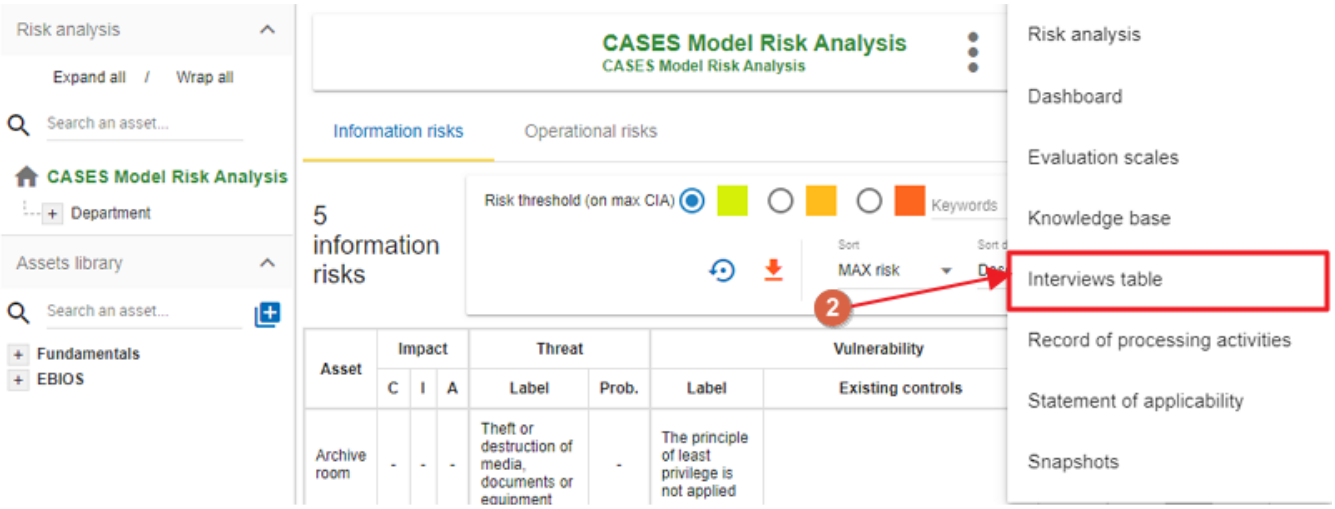
The Interviews table is used during risk analysis to document the various interviews conducted to gather information for the final report. Key details such as dates and interviewees can be included, ensuring a comprehensive and organized report.

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

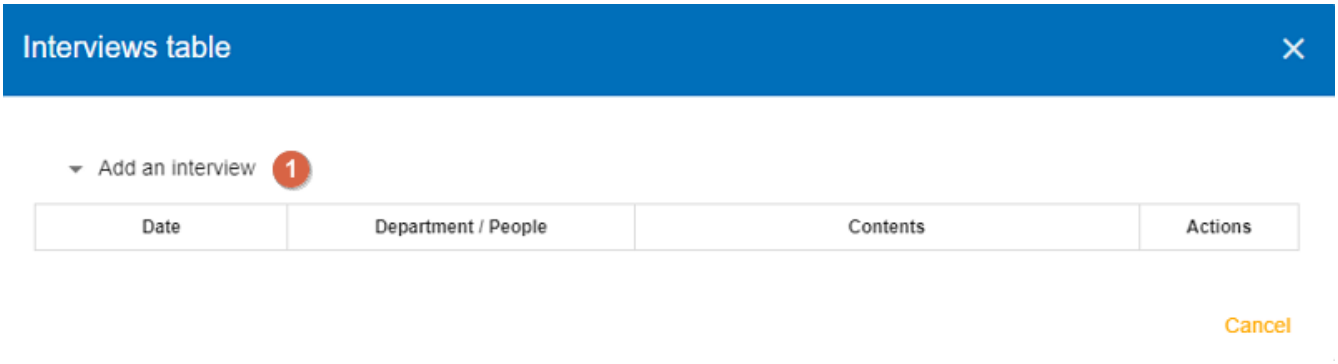
1. To reach the Interviews menu, first, click on the contextual menu ⋮ in the upper right-hand corner.



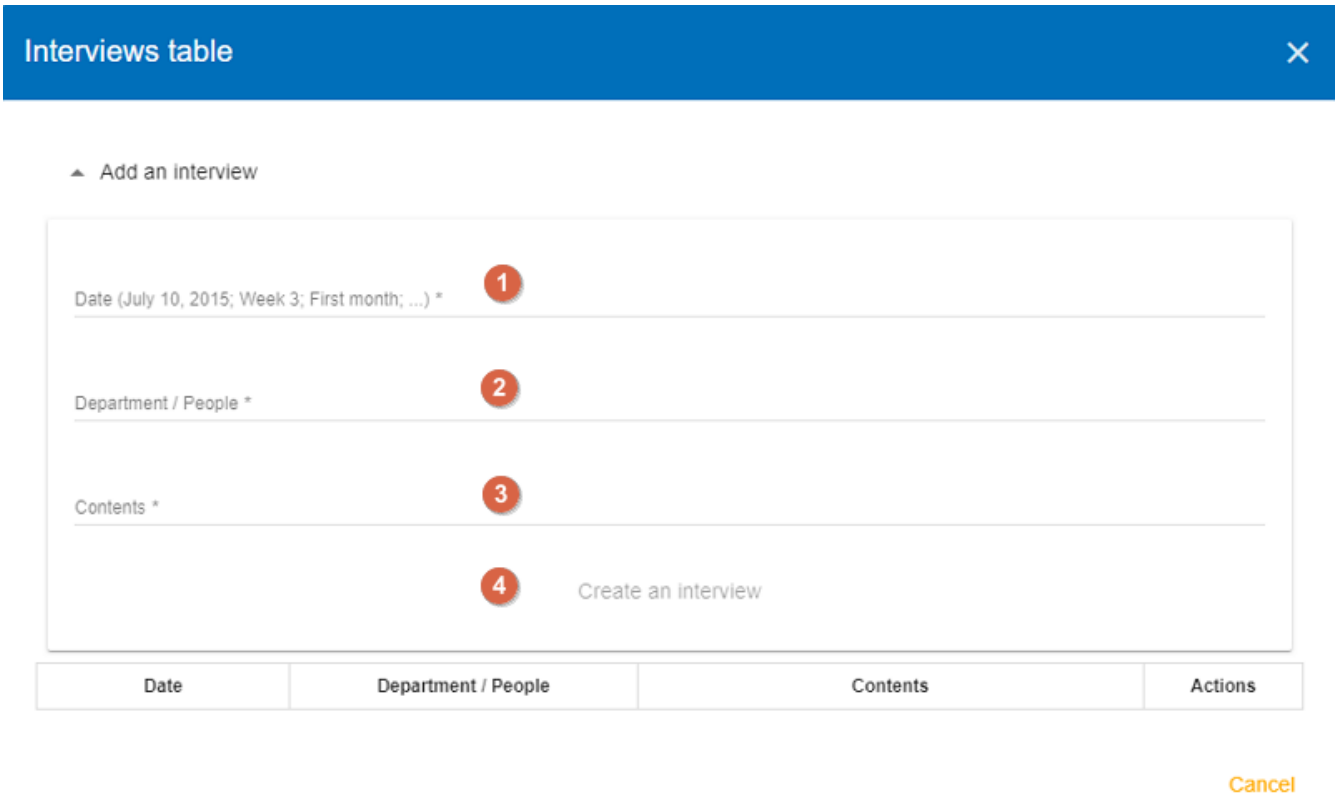
1. Then, from the dropdown-menu, choose the menu `Interviews table`.



1. Click on the link `Add an interview`.

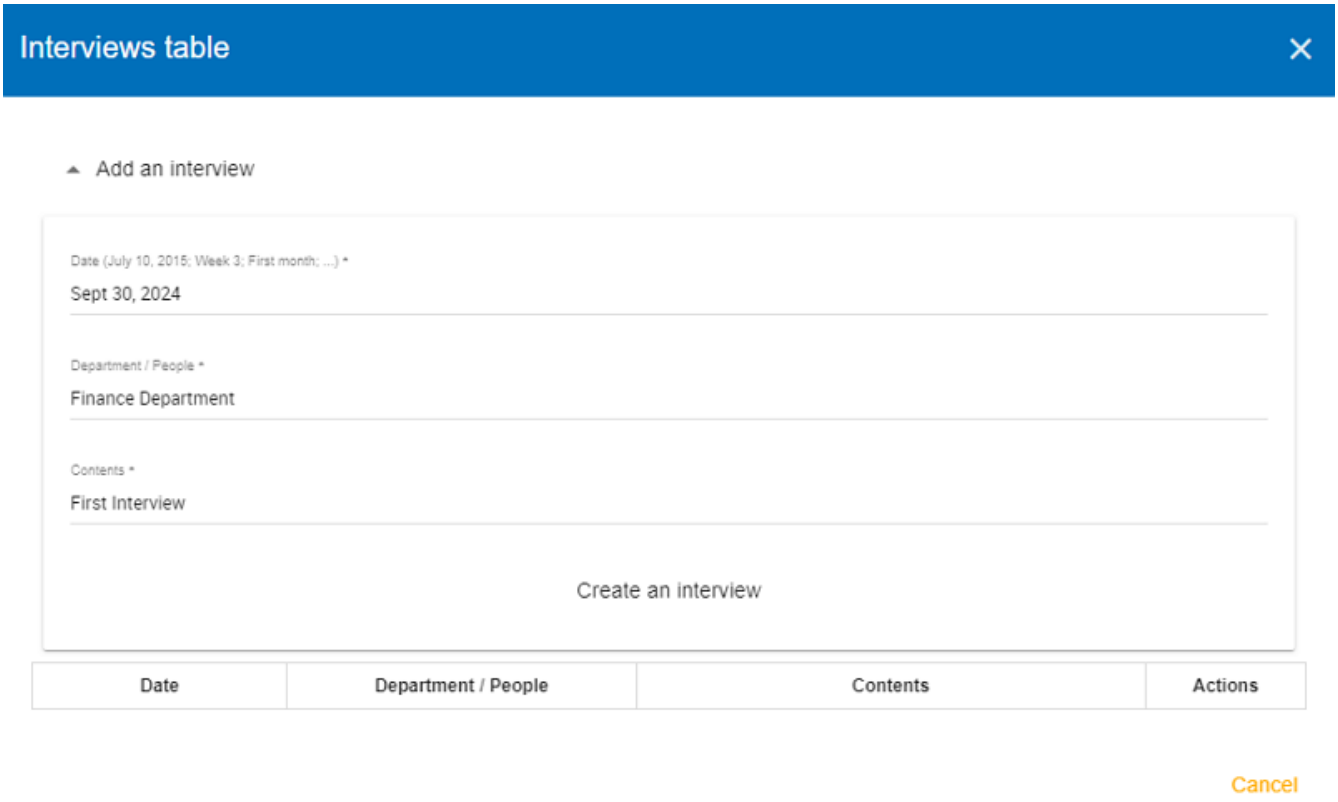


1. The `Interviews table` window opens.

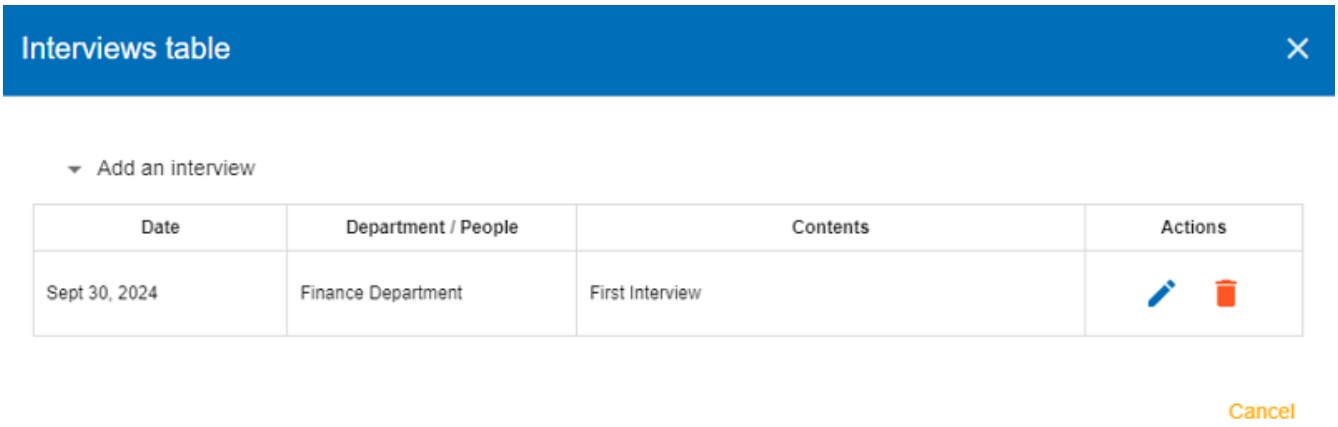


Some information has to be entered

1. Fill out the `Date`.
2. Give the `Names` of the people or the name of the department participate in the interview.
3. Enter the `Contents` covered.



Once all the fields are filled, click on the link `Create an interview`. The Interview table popup appears with the data you provided in the previous screen.



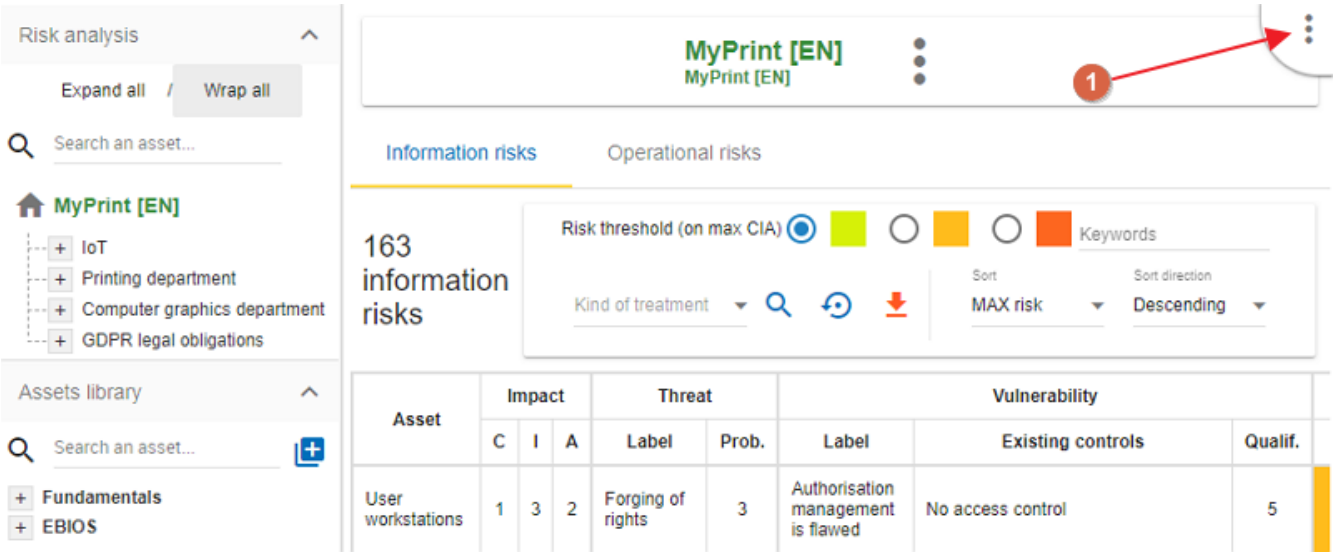
Chapter 13. Snapshots

Snapshots allow you to create a full backup for analysis.

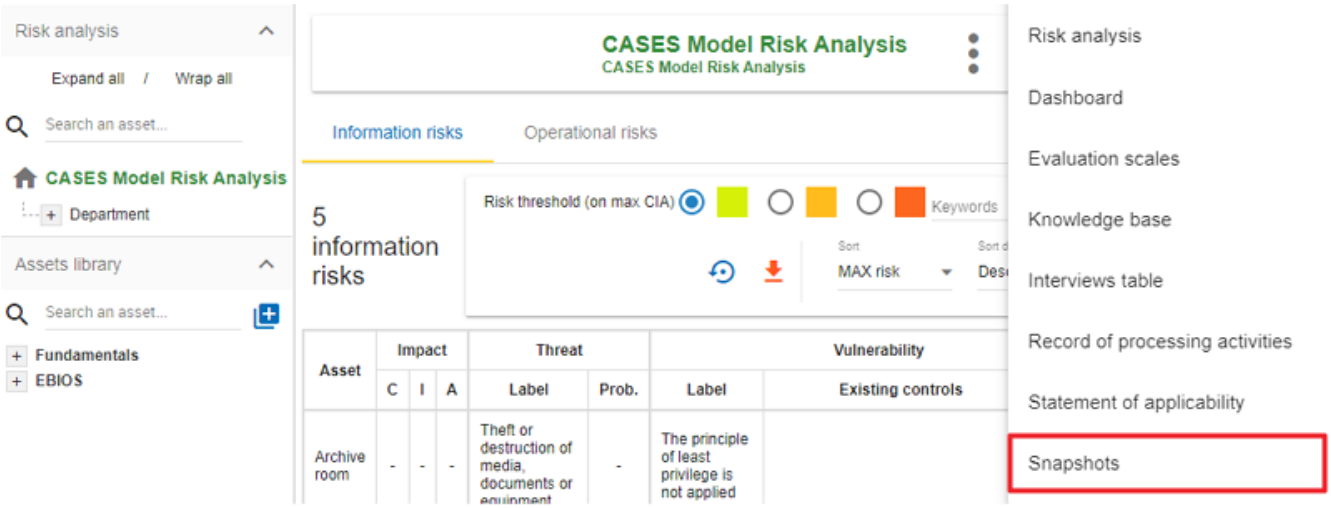
> It is a function to be used regularly throughout the process, both before and after major changes, as it provides the only way to track and reference those changes.

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

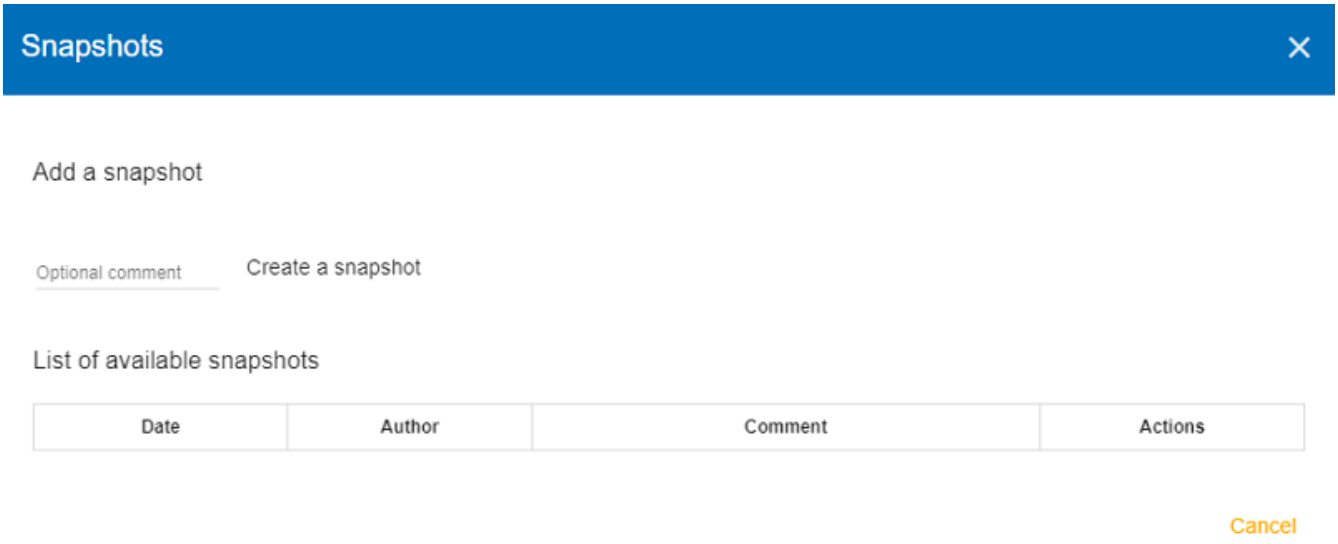
To reach the Snapshot functionality, first, click on the contextual menu ⋮ in the upper right-hand corner.



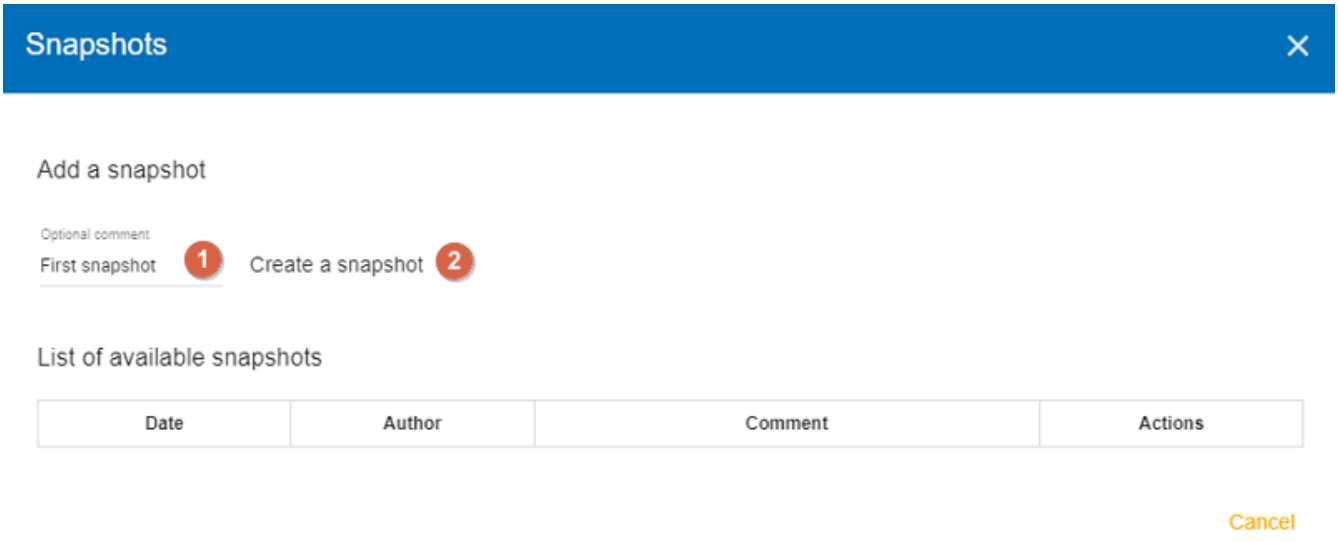
Then, from the dropdown-menu, choose `Snapshots`.



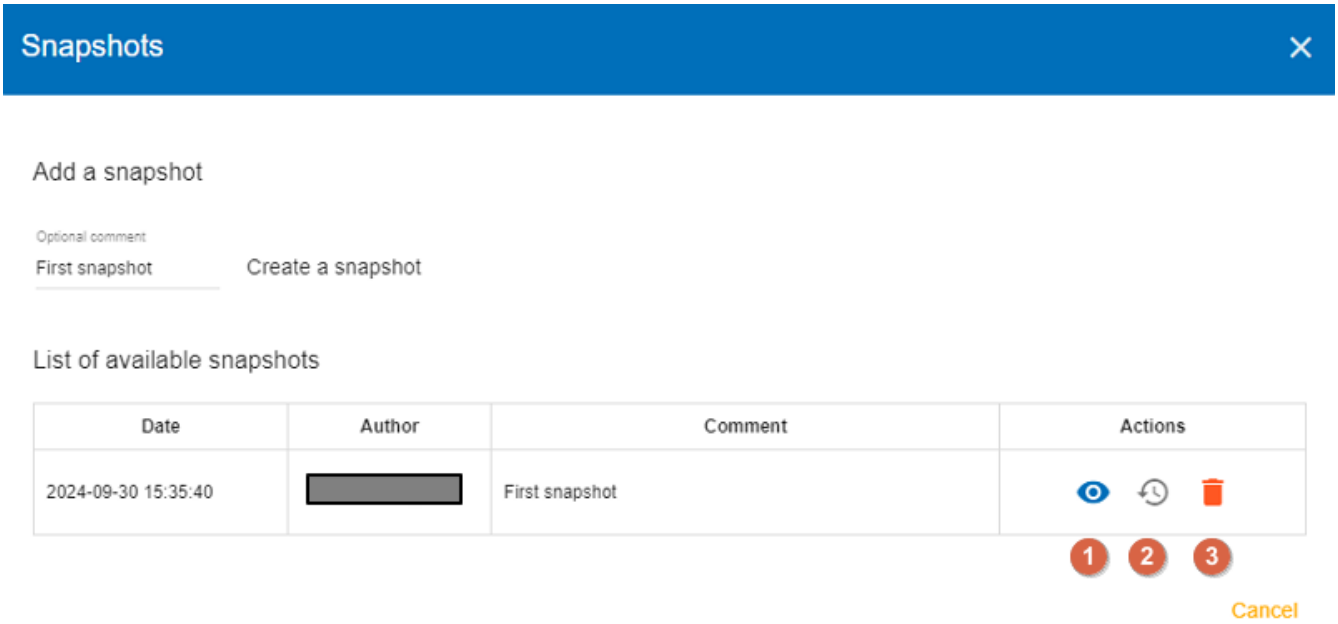
The following pop-up appears:



First, name your snapshot, then click on ‘Create a snapshot’ so you can create a backup of your project.



Once you clicked on ‘Create a snapshot’, the following screen appears showing the date and time when you created the snapshot. The table also shows your name and your comment (if you add a comment in the previous screen).

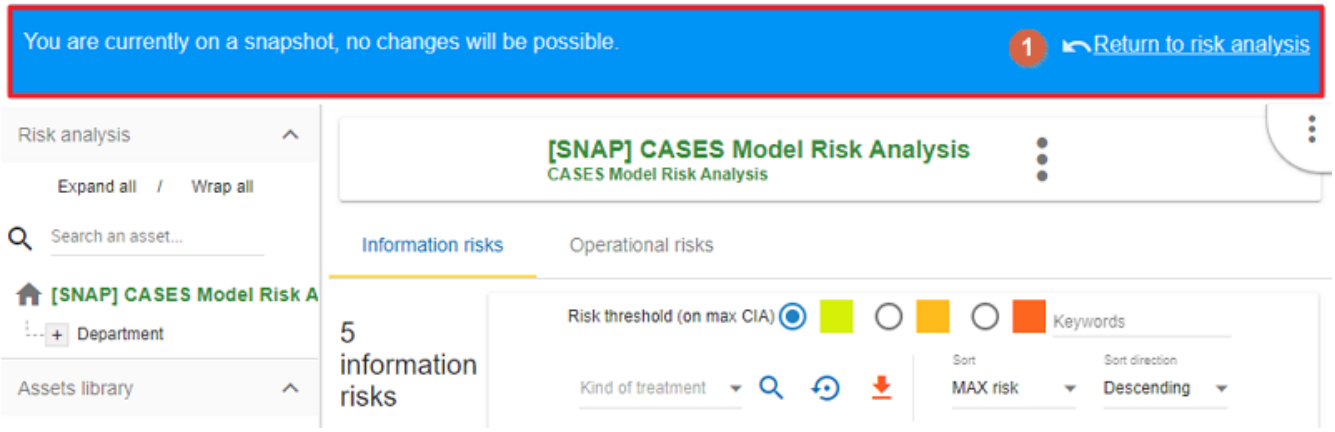


You can do the following actions:

1. `View` the snapshot
2. `Restore` the snapshot. Caution: this option will overwrite the current analysis!
3. `Delete` the snapshot you created.

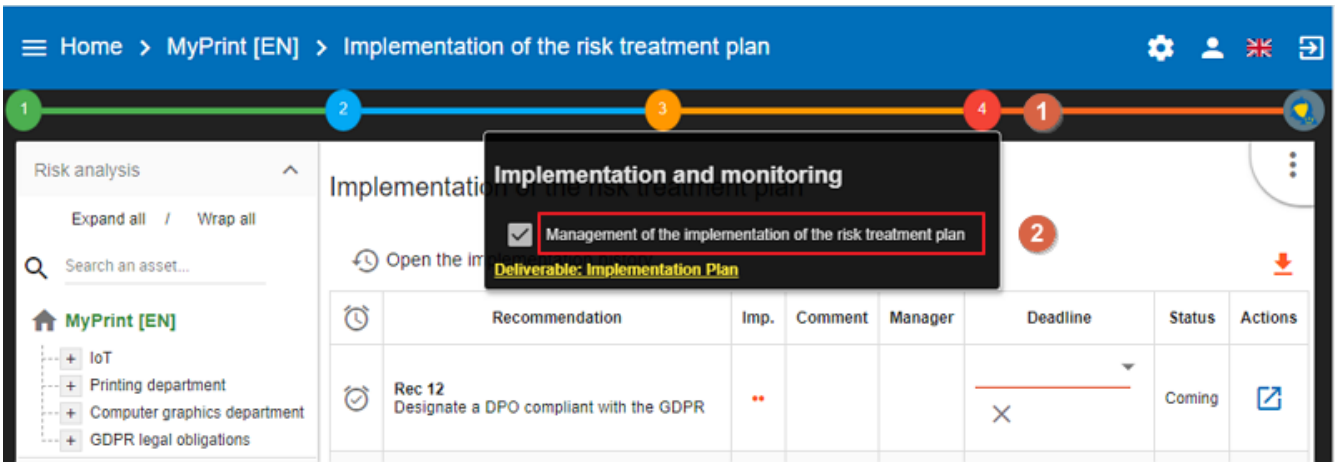
When you leave the popup window by clicking on the 'X' in the upper right-hand corner, you will see the snapshot view. A message informs you that you are curently on a snapshot and you cannot make any changes.

Click on the 'Return to risk analysis' link to back to your risk analysis.

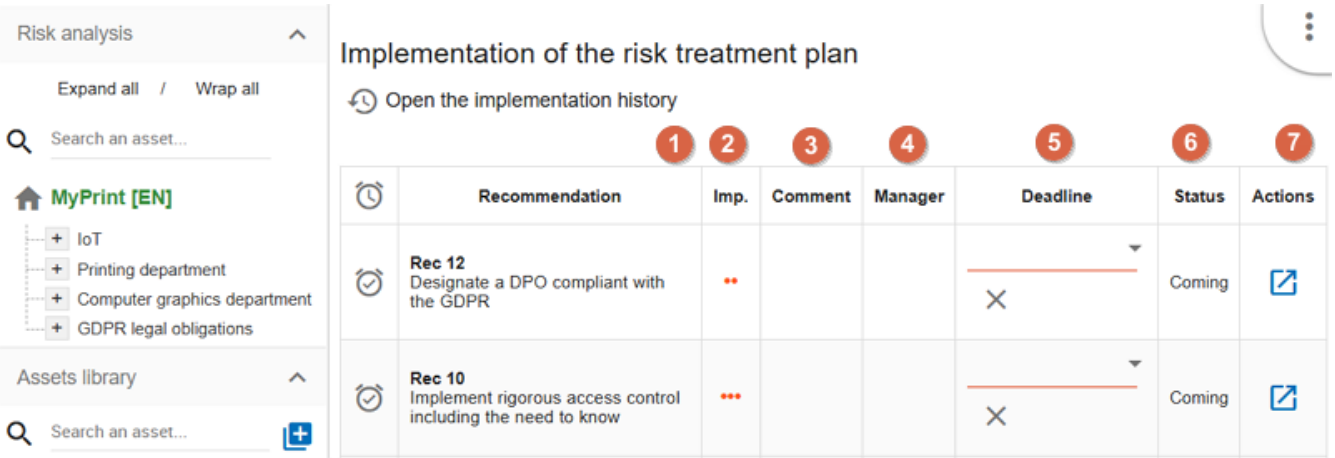


Chapter 14. Managing the Implementation Treatment Plan

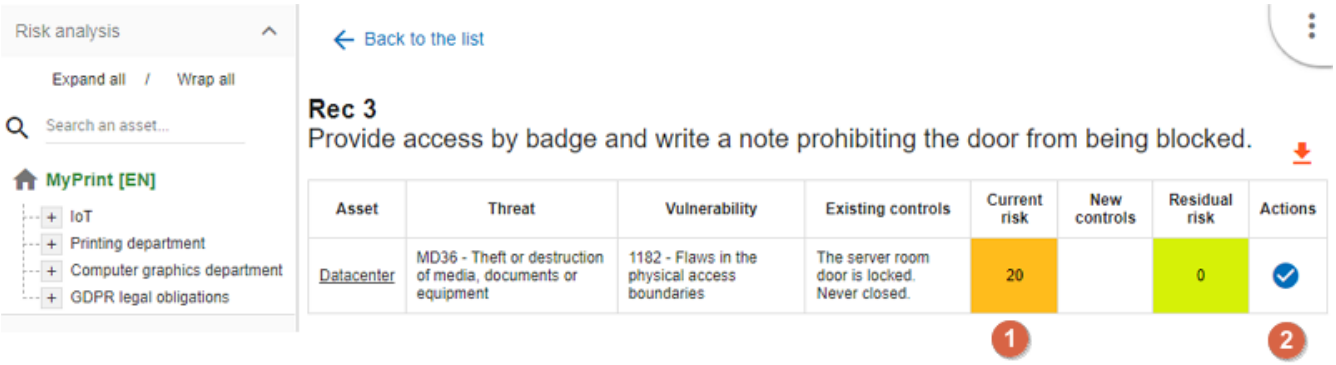
To create an Implementation and Treatment Plan, first click on number 4, then click on the link 'Management of the implementation of the risk treatment plan' in the popup appears:



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



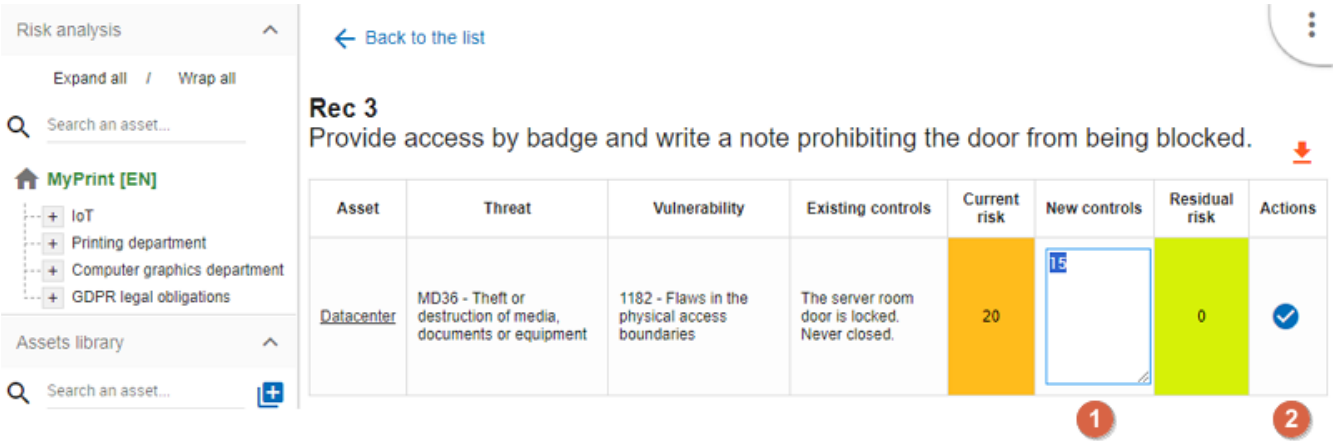
1. This is a `recommandation` established before.
2. Importance
3. You can put a `comment` for the implementation of the recommendation.
4. For each recommendation you can set a `manager`.
5. For each recommendation you can set a `deadline`. By clicking on the down-pointing triangle (in the upper right corner of the cell), you can open a calendar and set a different deadline.
6. `Status` of Implementation.
7. In the Actions column, click on the relevant icon to implement the recommendation and switch on the following view. By clicking on the icon in the second row (Rec 3), the following screen appears:



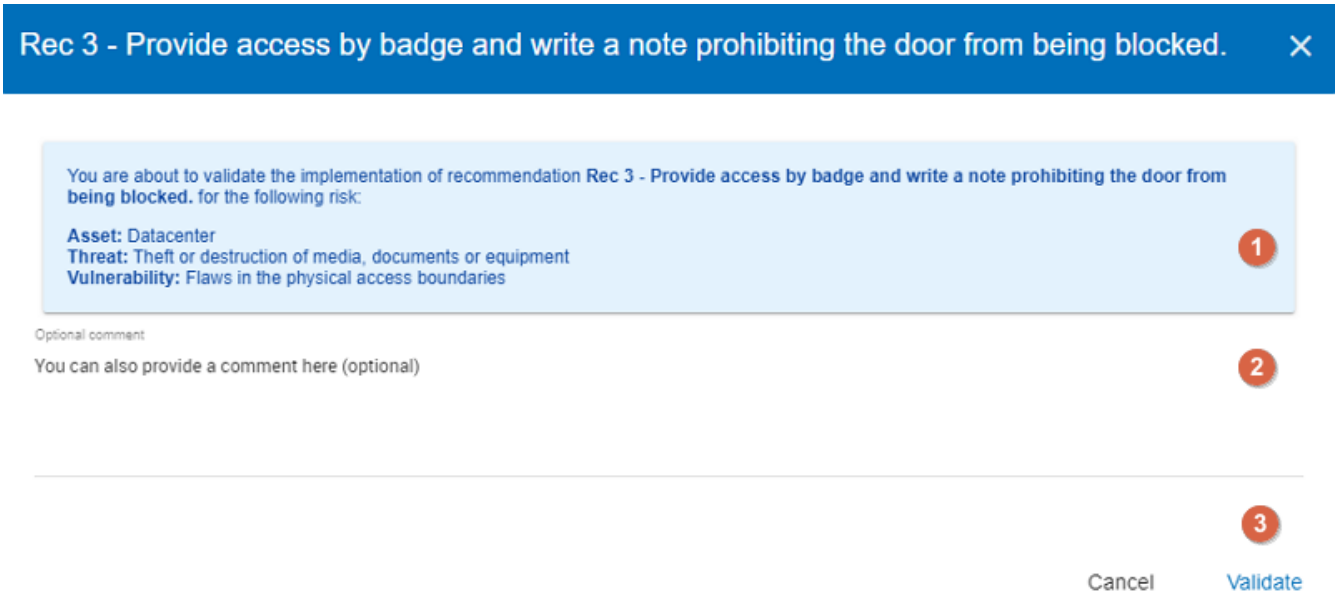
The screen provides information on the chosen asset, the threat and the vulnerability related to it, and the controls already implemented. You can set a new control (1) and launch the validation of it by clicking on the checkmark icon.

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

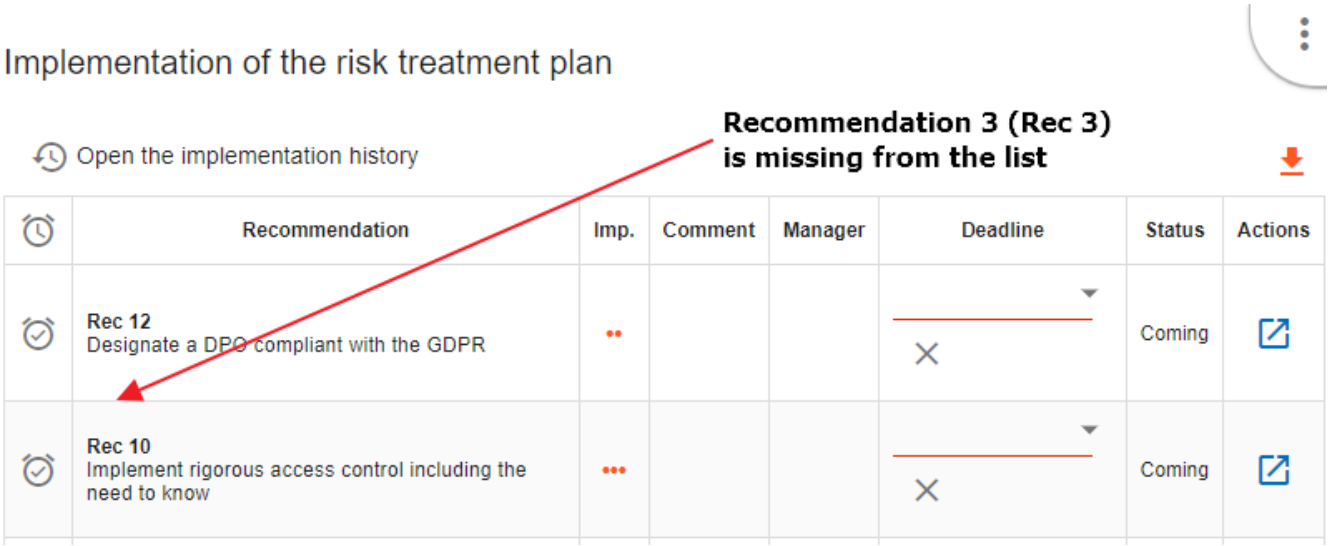
To set a new control, click inside the cell in the column 'New controls' and give a new value (1), then click on the checkmark (2) to validate it.



The following popup appears. At the top of the window, (area bounded on a blue background) you can read the summary about the asset, the threat and the vulnerability. Below, you can add an optional comment. As the final step, click on the 'Validate' link to save your changes.



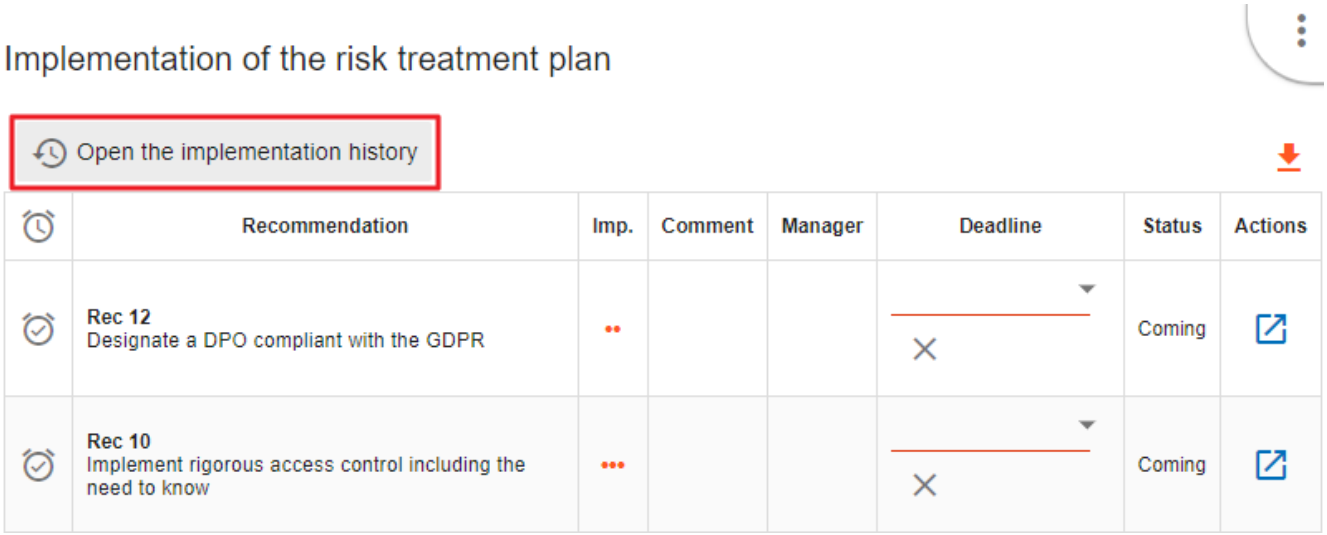
Once you click on the Validation link, the application takes you back to the 'Implementation of the risk treatment plan' screen. The changed recommendation (Rec 3) is removed from the list.



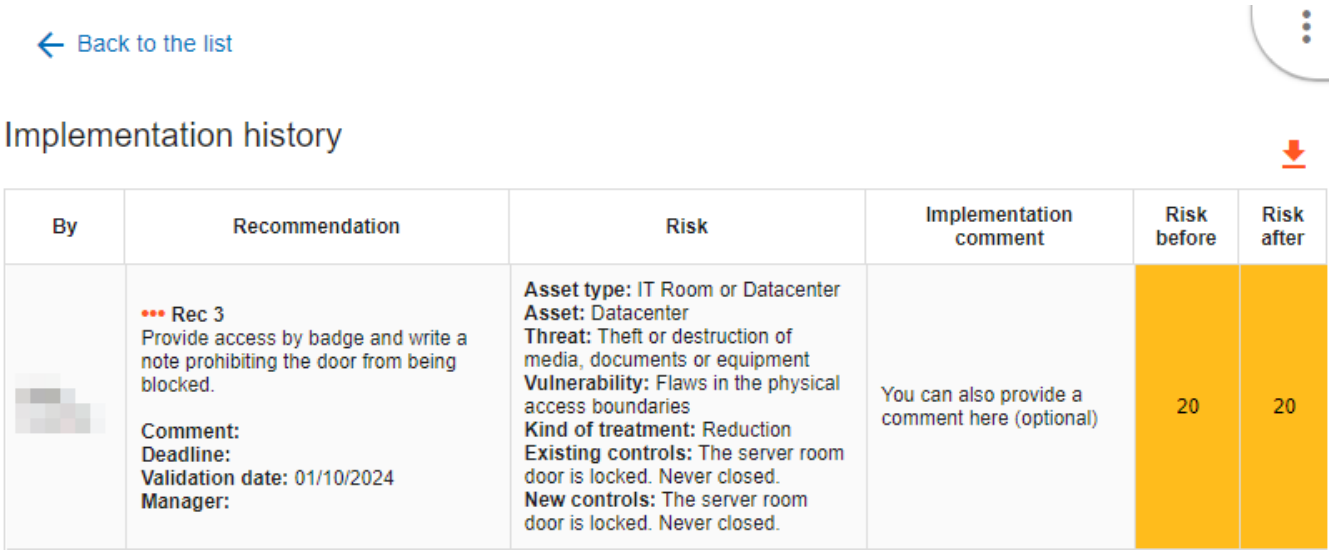
Now, you can follow the same procedure for each recommendation. After that go to your risk analysis and make a second iteration.

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. Click on the link 'Open the implementation history' to get a list of those recommendation you have already handled. Since I only modified one recommendation (Rec 3), there is only one item on the list:



The table shows all relevant data regarding the past recommendations. You can go back to the 'Implementation of the risk treatment plan' if you click on the 'Back to the list' link in the top left-hand corner. Click on the orange down-pointing arrow to export this table in CSV format.



The risks treatment table preparation is an important step before starting the implementation of the risks treatment plan. The goal is to prioritise the recommendations list by drag-and-drop and move the most important recommendations to the top of the list.

The risk treatment table's useful feature is the possibility to export the prepared list as a .csv file and update the recommendation codes and descriptions on place in case of needs.

Chapter 15. Global Dashboard

1. **Overview**

The Global Dashboard interacts with data stored on the Stats Service. It collects statistics for all existing analyses of the instance daily and sends them to the Stats Service, where they are stored in the database. If an analysis is removed, the corresponding statistical data is also deleted from the Stats Service database. For more details on installing the Stats Service, please refer to our **Technical Guide**,

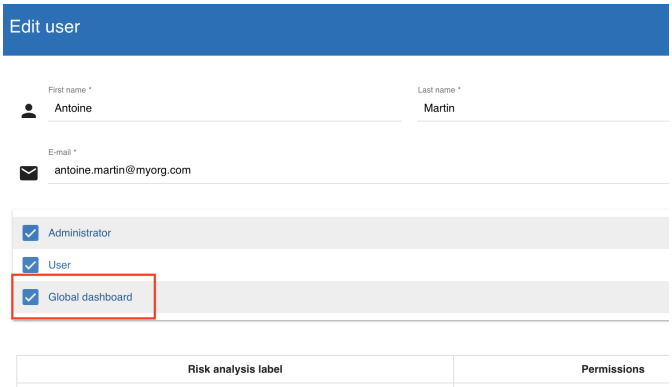
The Stats Service can send anonymized statistical data (with no client or instance identifying information) to a central repository called **Global Statistics**. The architecture of the services is available **here**. By default, statistics sharingcis enabled and is intended to assist the Monarc community in the future **forecasting**. However, this statistics sharing can be disabled (see point 5 - Global Dashboard statistics sharing option).

2. **Global dashboard access**

The Global Dashboard can be accessed from the Home page of Monarc. There are two types of the access, depending on the account privileges:

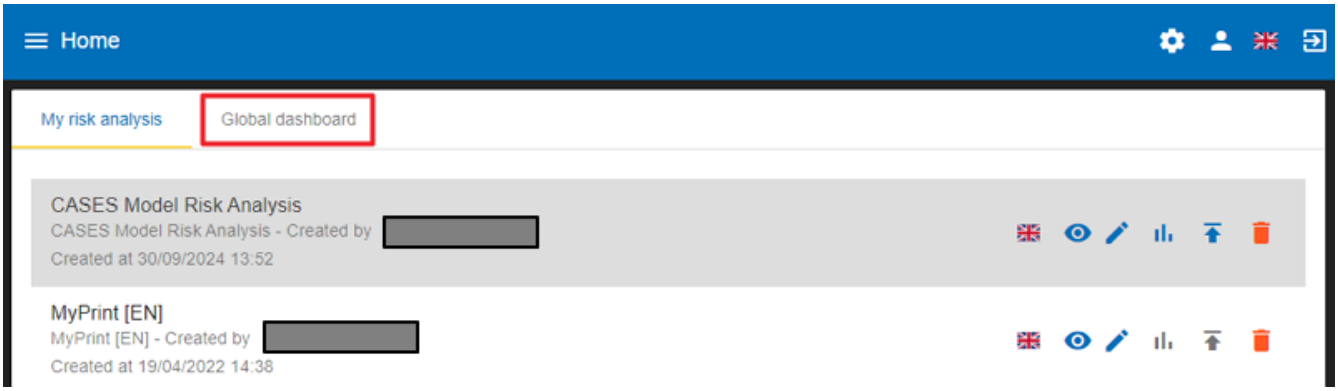
- If the account has "User" or "Administrator" permissions, the user will only be able to view statistics for the analyses they have access to.
- If the account has "Global Dashboard" permission, the user can view statistics for all analyses within the instance. There is also an option to configure the visibility of analyses (see number 2 in the yellow box).

3. **Global Dashboard access account setting**



4. **Home page access**

The Global Dashboard tab is visible on the Home page only if at least one analysis exists and the Stats Service is set up.

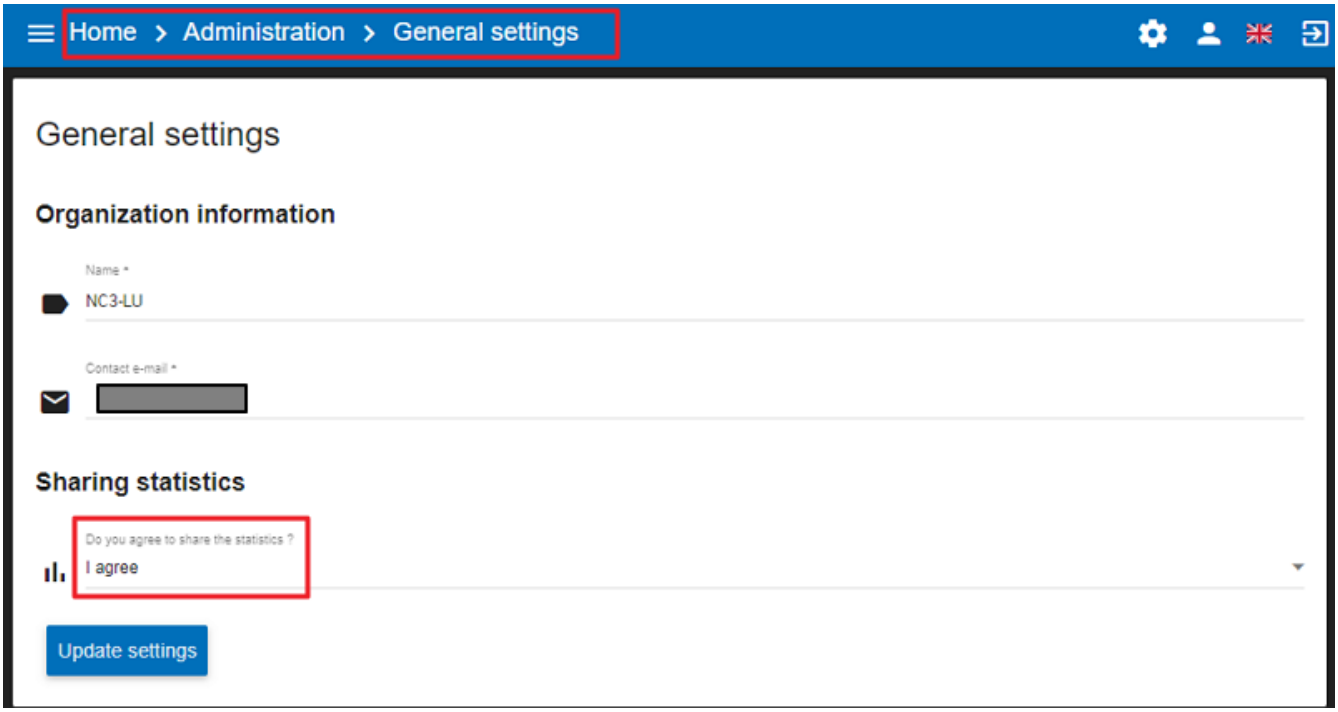


The Dashboard contains the analysis and the following icons to manage them:

1. Language
2. Read and Write access (an eye icon)
3. Edit the Dashboard
4. Visible (blue icon) or not visible (grey icon) on the Global Dashboard
5. Statistics data is collected (blue icon)/ommitted (grey icon)

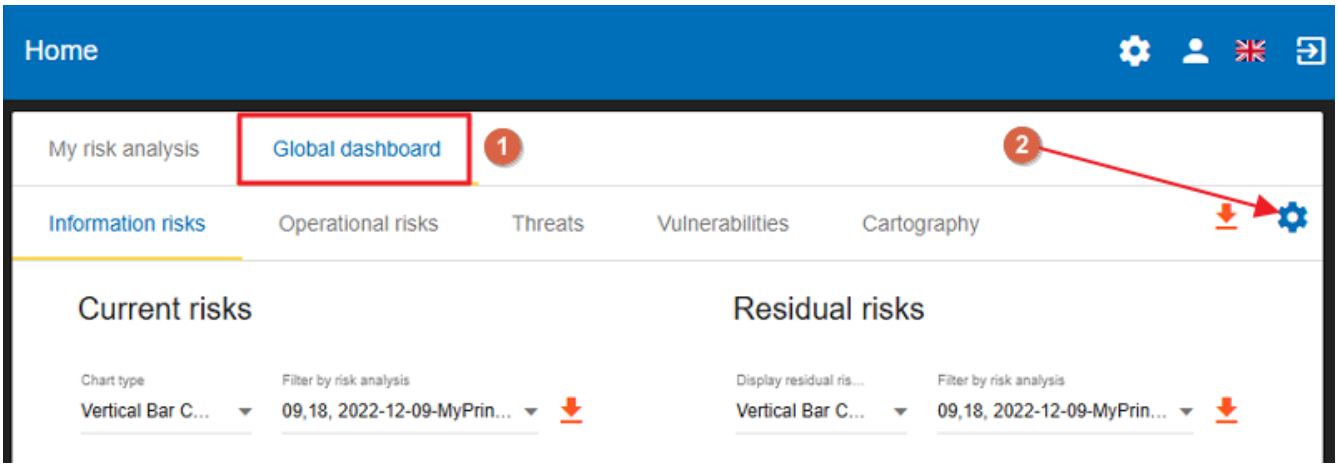
5. **Global Dashboard statistics sharing option**

As shown in the screenshot below, you can disable statistics sharing for your instance. Click the gear icon on the Home page, and choose ‘General settings’.

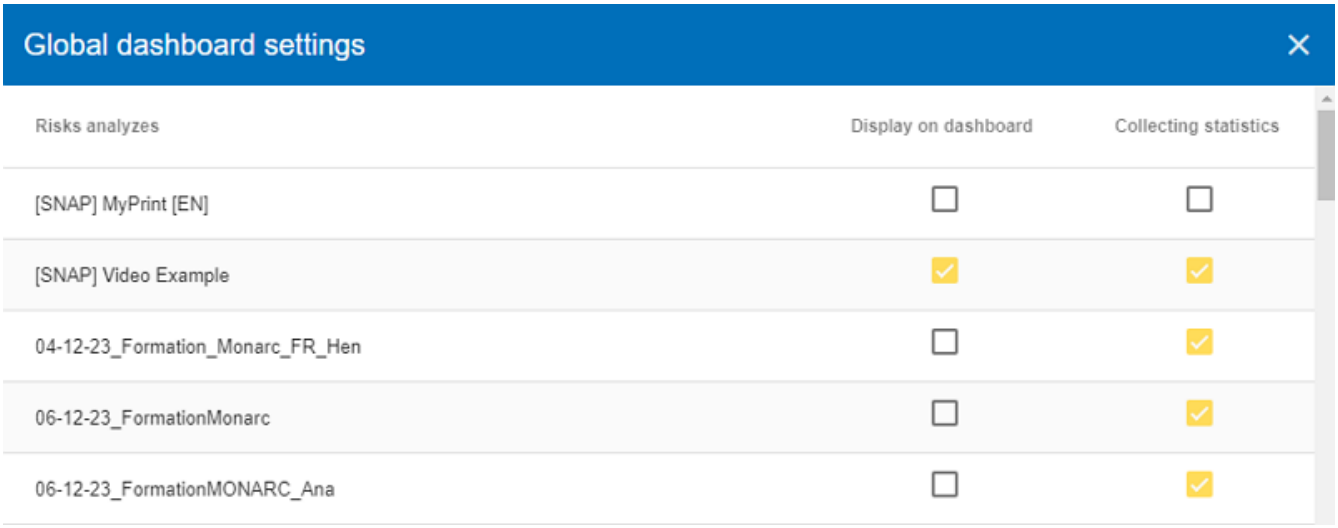


6. **Global Dashboard analyzes visibility setting**

This option is accessible only to accounts with "Global Dashboard" permissions and can be found in the top-right corner of any Global Dashboard chart tab. Only the selected analyses will be displayed on the charts. On the Home page, click on the Global dashboard link, then on the gear icon (Settings) in the top right-hand corner:

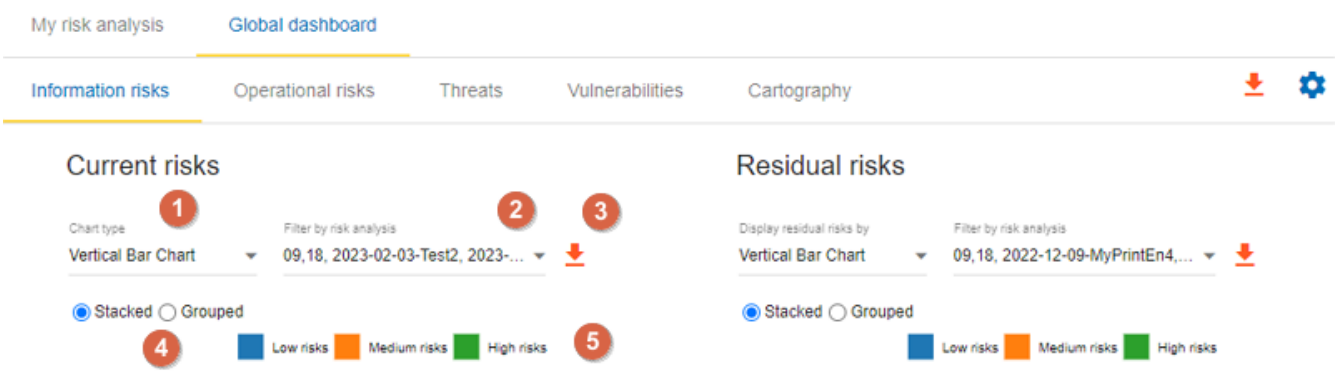


The Global Dashboard settings page will appear, allowing you to decide for each risk analysis whether you want it to be displayed on the dashboard and whether statistics should be collected for it.

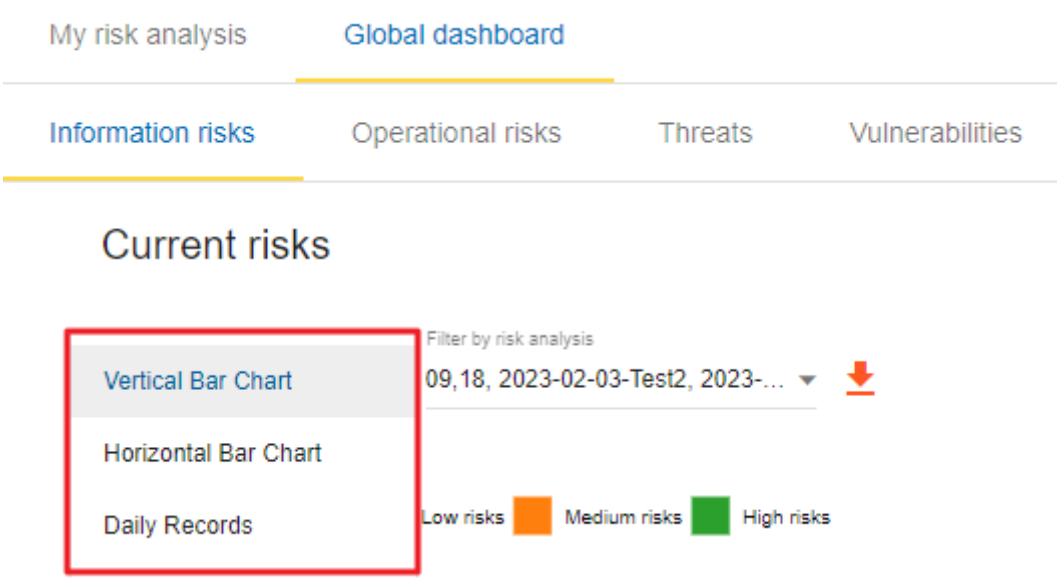


7. **Global Dashboard statistics overview**

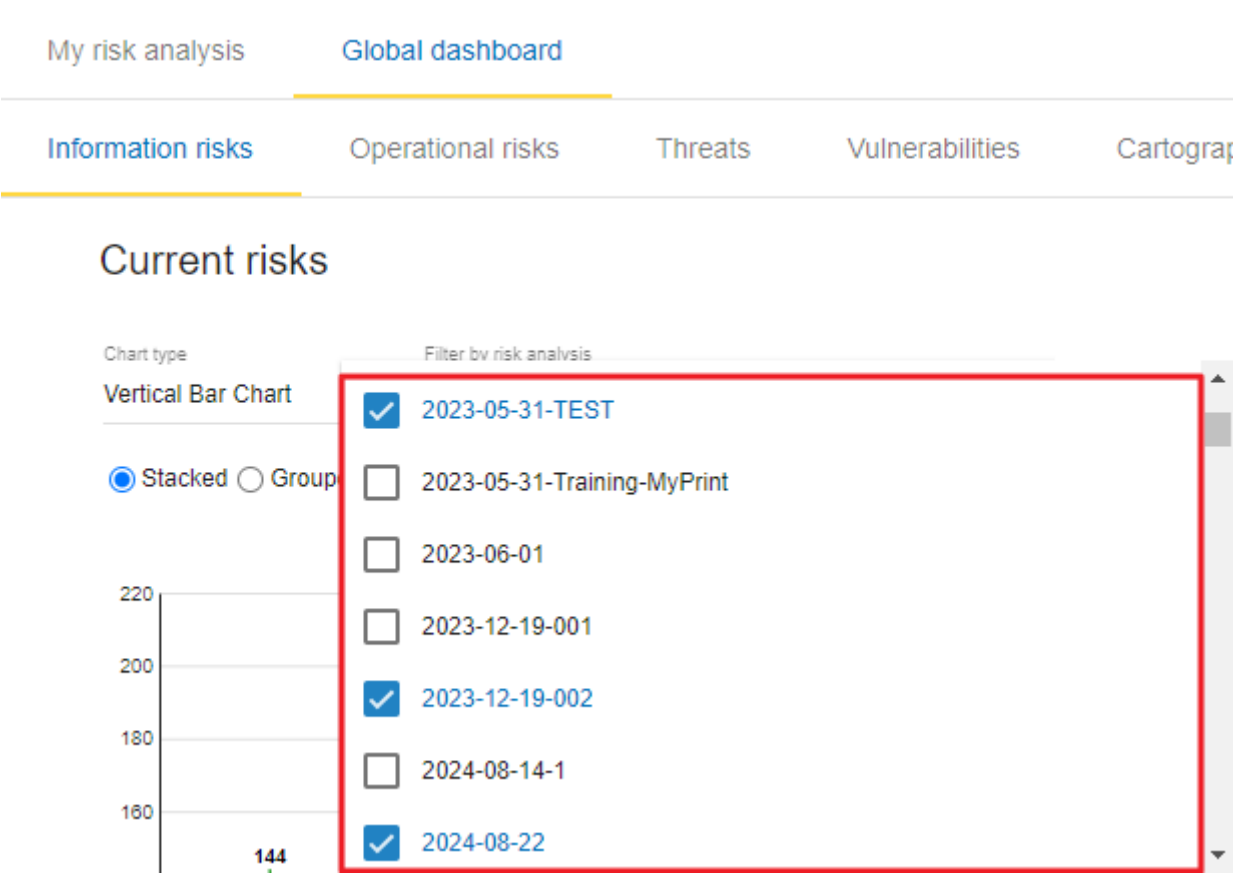
On the left, you can see the Current risks analyses, whereas on the right, the Residual risks analyses.



Decide what kind of chart type you want to get Vertical Bar Chart, Horizontal Bar Chart, or Daily Records)



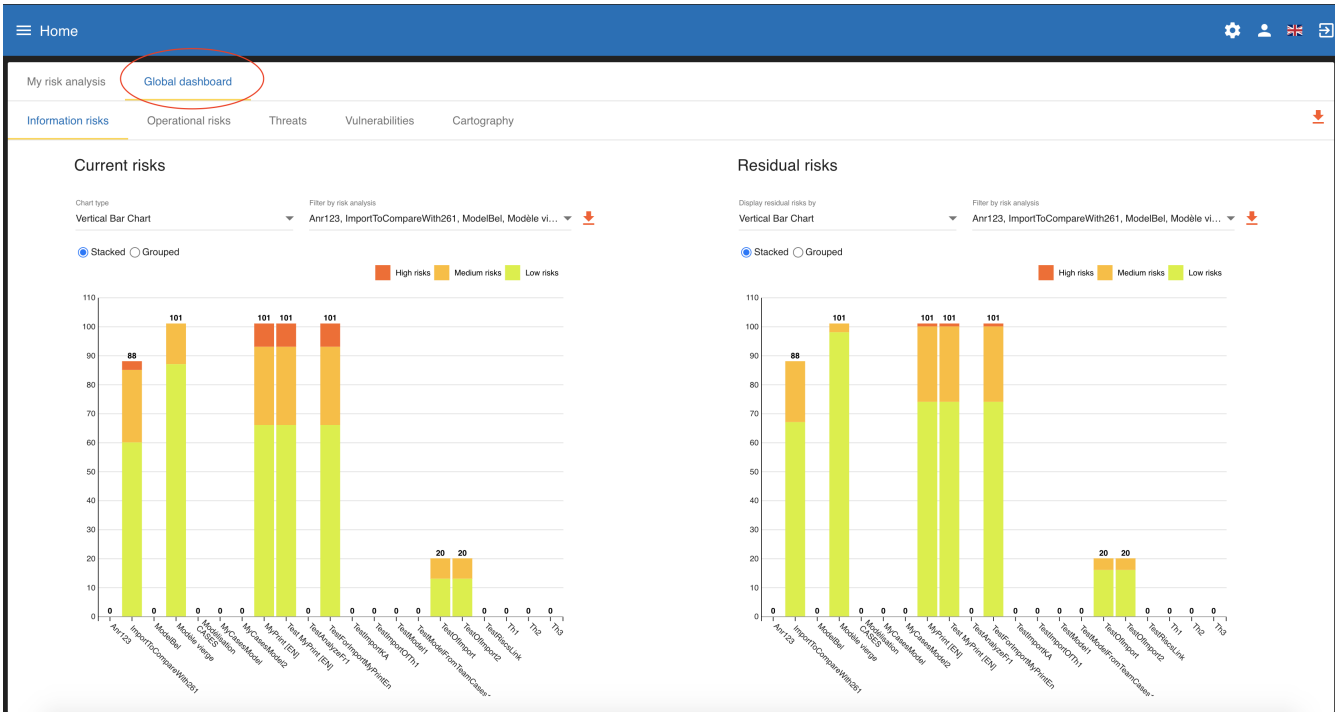
Filter by risk analysis: You can decide wich risk analysis should be shown on the Dashboard



1. You can export the chart as a PNG file
2. You can decide whether you want to see the risks stacked or grouped on the chart
3. By ticking the checkbox in front of them, you can decide whether you want to see the Low risks, Medium risks or High risks (or all of them)

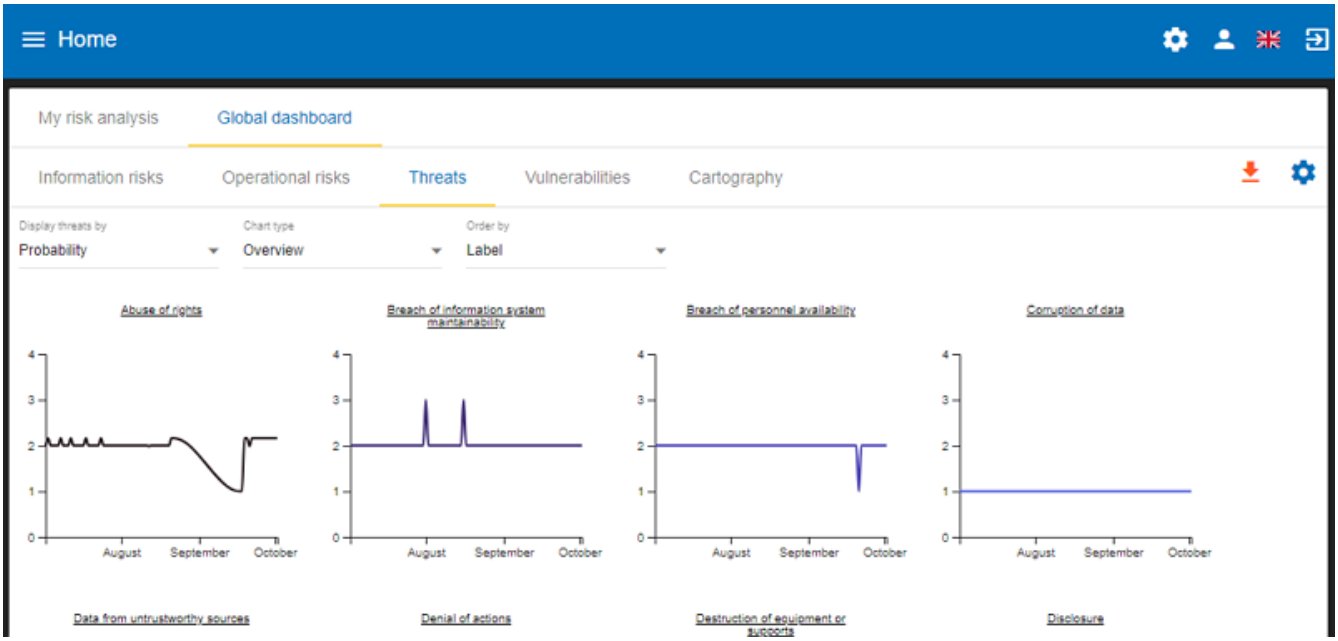
In the below screenshot, only the medium and high risks are shown on a vertical bar chart:

Here are some examples of charts generated from comparisons of different analyses. * **Informational risks**. The stats represents comparison of the informational risks of all the available analyzes.



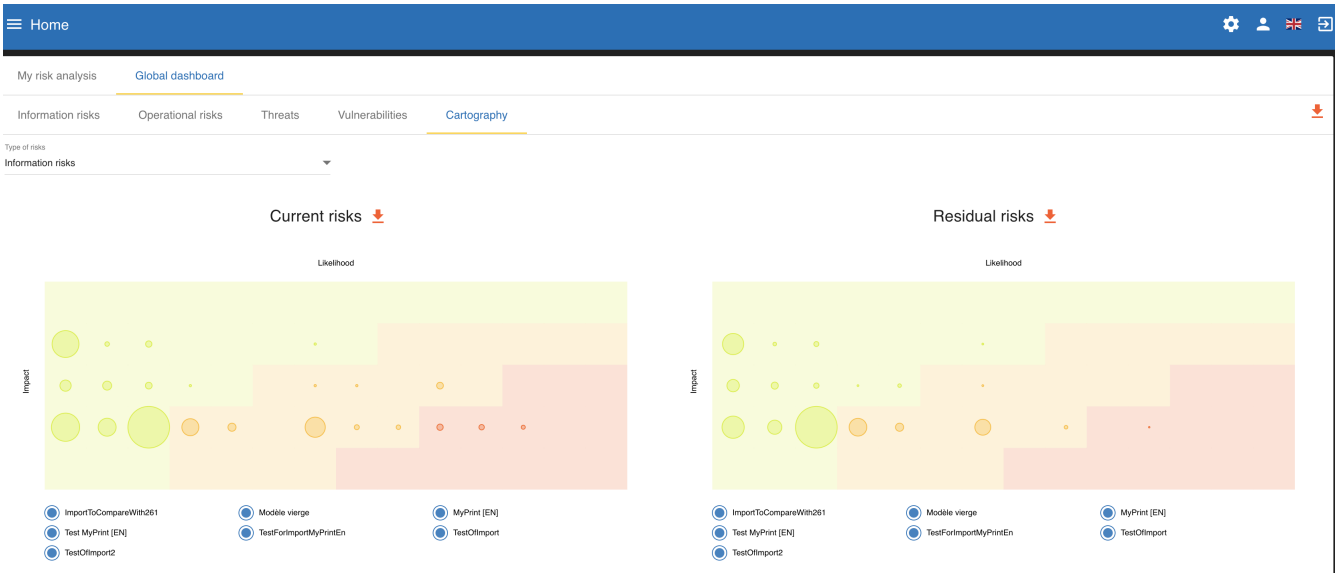
- **Operational risks**. The stats represents comparison of the operational risks of all the available analyzes.

- **Threats**. Threats can be shown as per their probability, occurrence, or their maximum associated risk level as an overview or as per a daily records view. You can also filter among the threats by providing a start and end date and you can export the charts as a PNG file.



- **Vulnerabilities**. The vulnerabilities overview shows vulnerabilities as per their qualification, occurrence, and Max. associated risk level.

- **Cartography**. Matrix with the average analyzes levels based on impact and likelihood.


Home
My risk analysis
Global dashboard
Information risks
Operational risks
Threats
Vulnerabilities
Cartography
Type of risks
Information risks
Current risks
Likelihood
Impact
ImportToCompareWith261
Modèle vierge
MyPrint [EN]
Test MyPrint [EN]
TestForImportMyPrintEn
TestOfImport
TestOfImport2
Residual risks
Likelihood
Impact
ImportToCompareWith261
Modèle vierge
MyPrint [EN]
Test MyPrint [EN]
TestForImportMyPrintEn
TestOfImport
TestOfImport2