OPTIMISED RISK ANALYSIS

www.monarc.lu

Method Guide

CASES Luxembourg

Table of Contents

1. Introduction . . . 1
   1.1. Purpose . . . 1
   1.2. Other documents . . . 1
   1.3. Syntax used in the document . . . 1
   1.4. Syntax used in MONARC . . . 1
2. Monarc Method . . . 1
   2.1. Iterative Method . . . 2
   2.2. Qualitative method . . . 3
   2.3. Method broadly based on ISO/IEC 27005 . . . 3
   2.4. Access to methodology screens . . . 4
   2.5. Details of the stages . . . 5
3. Context Establishment . . . 5
   3.1. Risk analysis context . . . 6
   3.2. Evaluation of the trends, threats and synthesis . . . 7
   3.3. Risks management organisation . . . 9
   3.4. Definition of the risk evaluation criteria . . . 10
   3.5. Deliverable: Context validation . . . 13
4. Context Modeling . . . 13
   4.1. Identification of assets, vulnerabilities and impacts appreciation . . . 14
   4.2. Summary of assets/impact . . . 15
   4.3. Deliverable: Validation of the model . . . 16
5. Evaluation and treatment of risks . . . 16
   5.1. Evaluation and treatment of risks . . . 17
   5.2. Risk treatment plan management . . . 18
   5.3. Deliverable: End report . . . 19
6. Implementation and monitoring . . . 19

1. Introduction

1.1. Purpose

The purpose of this document is to explain the procedures of the MONARC method by describing the various steps offered by the tool.

1.2. Other documents

- **Quick Start**: Provide a quick start with MONARC.
- **User Guide**: Complete documentation of the tool.
- **Technical Guide**: Complete technical documentation.

1.3. Syntax used in the document

All numbers in white on a red background are used on print-screen views to provide additional explanations. Explanations are always after the view with the corresponding numbering. **i.e.** 1.

`Reference`

MONARC Reference

1.4. Syntax used in MONARC

Button that always brings up the menu.

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

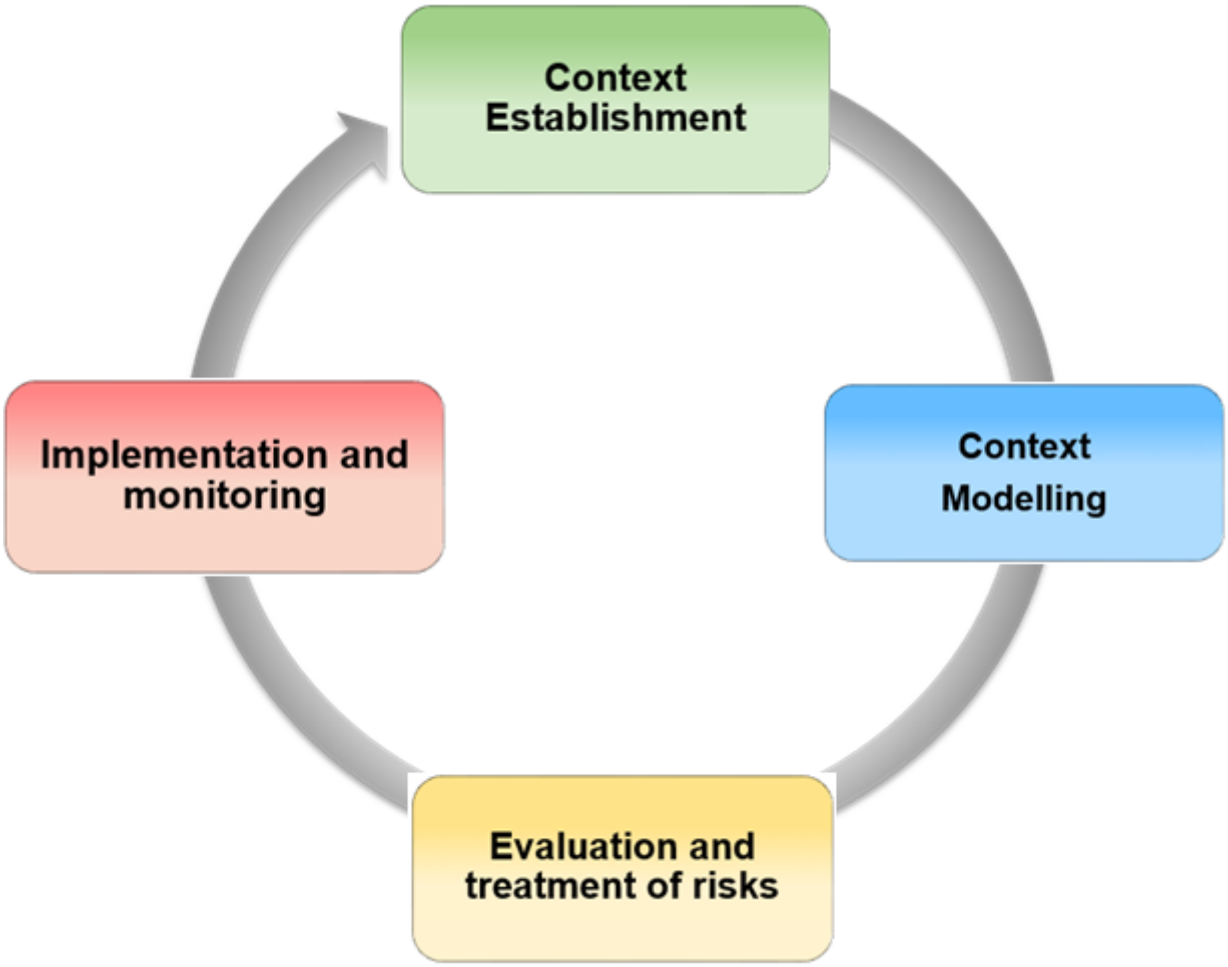
Most fields of MONARC display additional information when the pointer stay unmoved some time.

2. Monarc Method

MONARC is an iterative and qualitative method of risk analysis in four stages; broadly inspired by ISO/IEC 27005.

2.1. Iterative Method

MONARC uses an iterative method which enables the pragmatic progression of risk management. This approach, as recommended by ISO 27005, enables the user to restrict himself to the essentials, then to carry out successive iterations to broaden the target or further refine it to cover more technical aspects. The optimised risk models provided as standard with the tool will enable this type of management to be carried out.



1. `Context establishment`: Definition of the target of the risk analysis, establishing and describing the context, defining the risk analysis criteria and the structure of the risk approach.
2. `Context modelling`: Development phase of the risk model. After having identified the primary assets, they just need to be broken down into support assets on a priority basis. The most common assets are present in the MONARC knowledge base and therefore identification of risk by default is offered. This type of identification may be sufficient in an initial risk iteration; however, it is the responsibility of the risk expert to provide the comprehensive model.
3. `Evaluation and treatment of risks`: Risk assessment involves establishing the level of threats and vulnerabilities of the context type under review. The processing of risk entails proposing security measures which tend to lower major risks to acceptable levels and to accept low risks.
4. `Implementation and monitoring`: The current MONARC version provides a follow-ups views in terms of the implementation of recommendations. Monitoring involves checking the major changes to the risk analysis context on a regular basis, as well as any major changes beyond said context which would imply a redesign of an analysis iteration.

2.2. Qualitative method

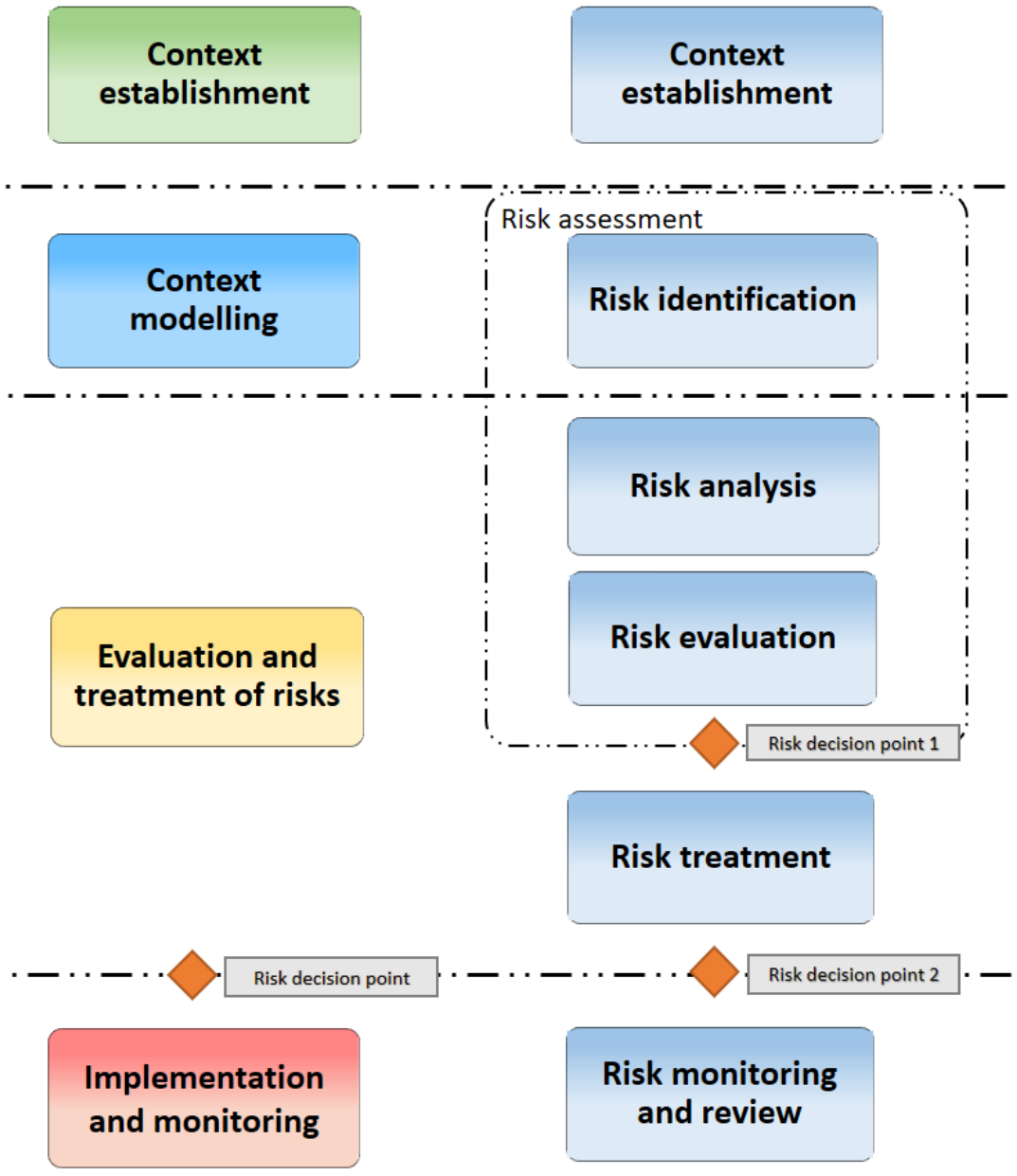
MONARC is a **Qualitative** method,

the risk parameters are determined on a contextual digital scale which enables the risks to be prioritised.

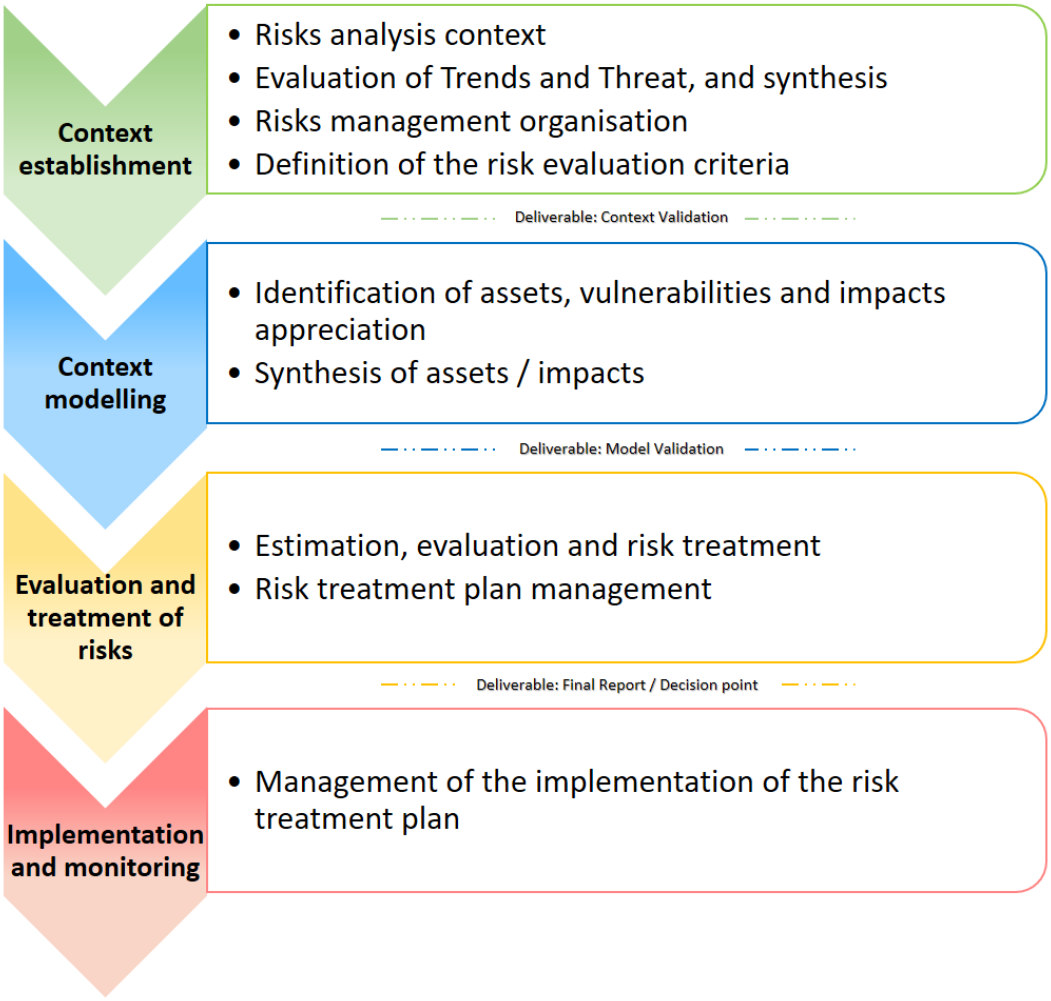
This approach is based on ISO/IEC 27005 as it is easier to understand, especially for non-tangible criteria in terms of impact and consequences, such as reputation, operational, legal, etc.

2.3. Method broadly based on ISO/IEC 27005

The illustration above displays the similarities between ISO/IEC 27005 and MONARC.

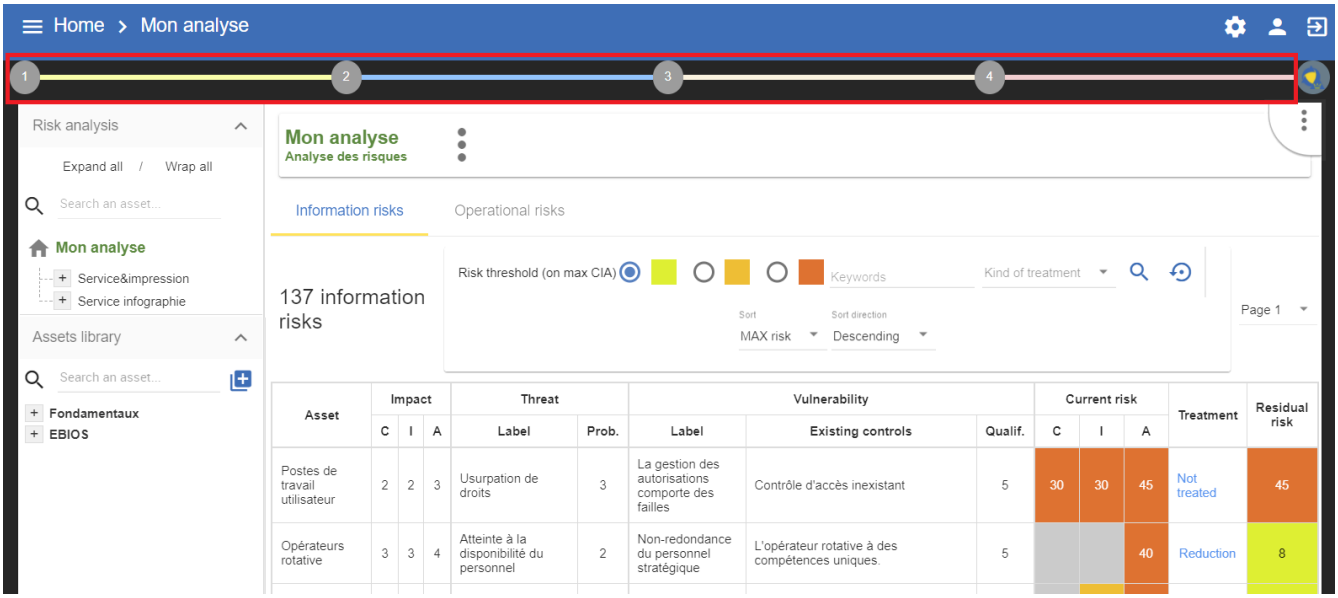


The sub-stages provided by the method are also in line with ISO/IEC 27005:

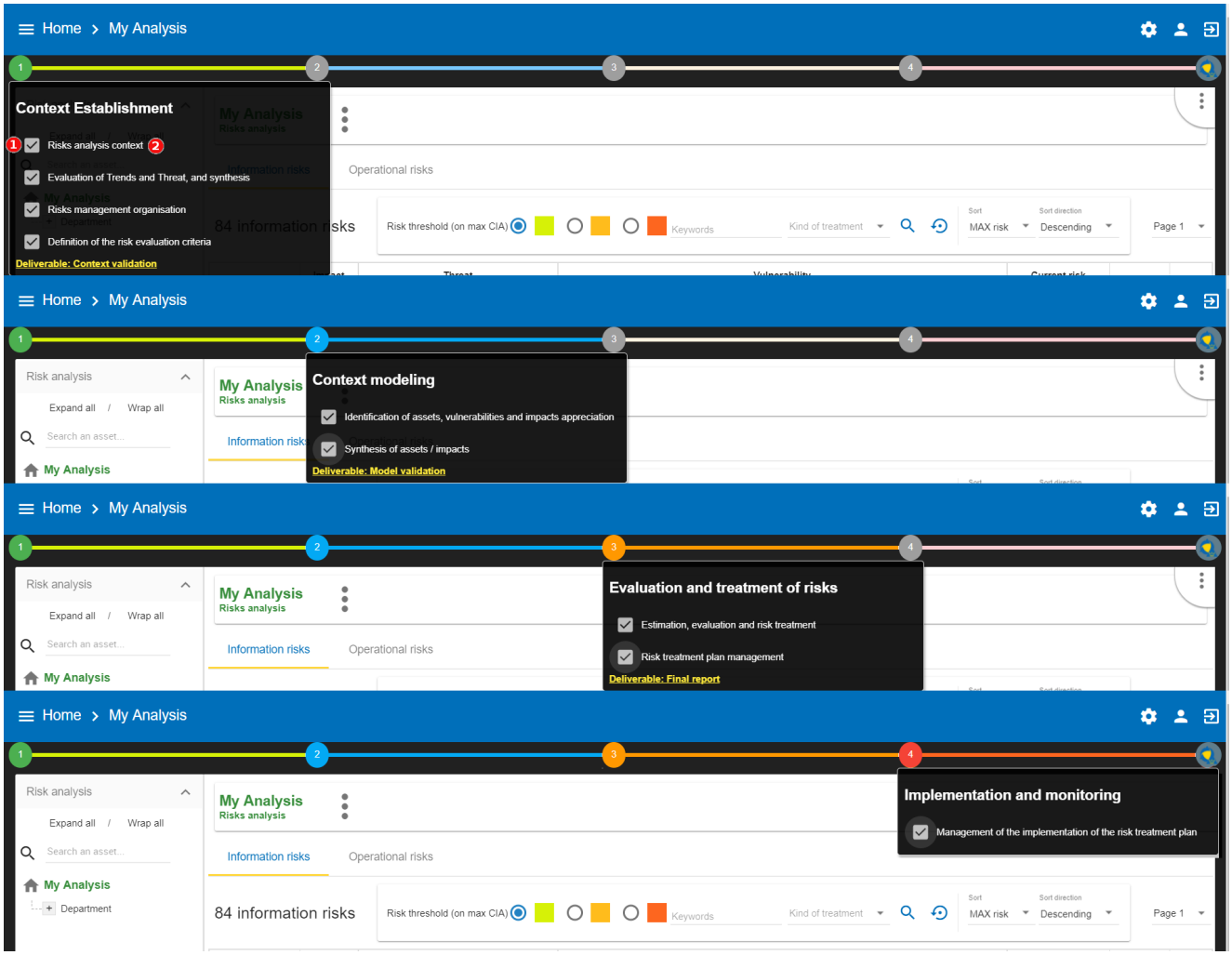


2.4. Access to methodology screens

Access to the views of the various stages of the method is provided by clicking on the numbers 1 to 4, which are displayed under the Breadcrumbs in the main MONARC view. The ISO/IEC 27005 processes are implemented via the views.



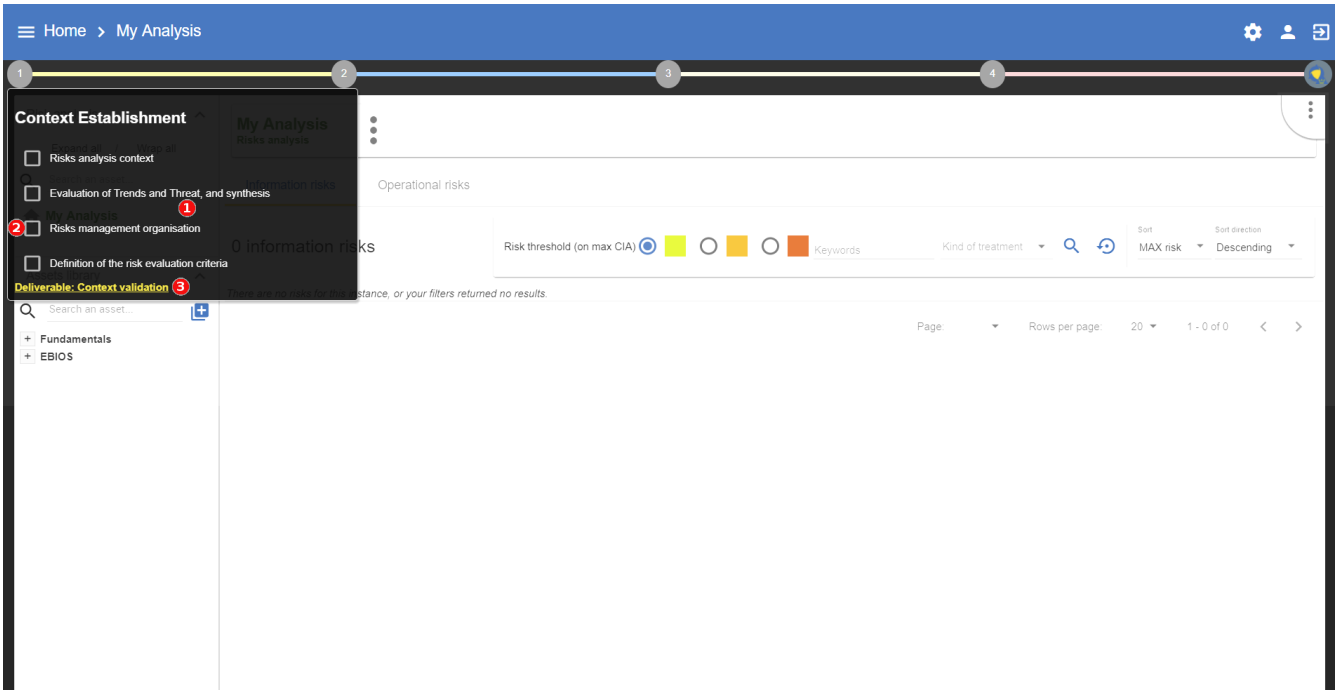
2.5. Details of the stages



1. Ticking the boxes enables the user to develop the progress status of the method
2. Clicking on the heading provides access to the management contextual sub-screen

3. Context Establishment

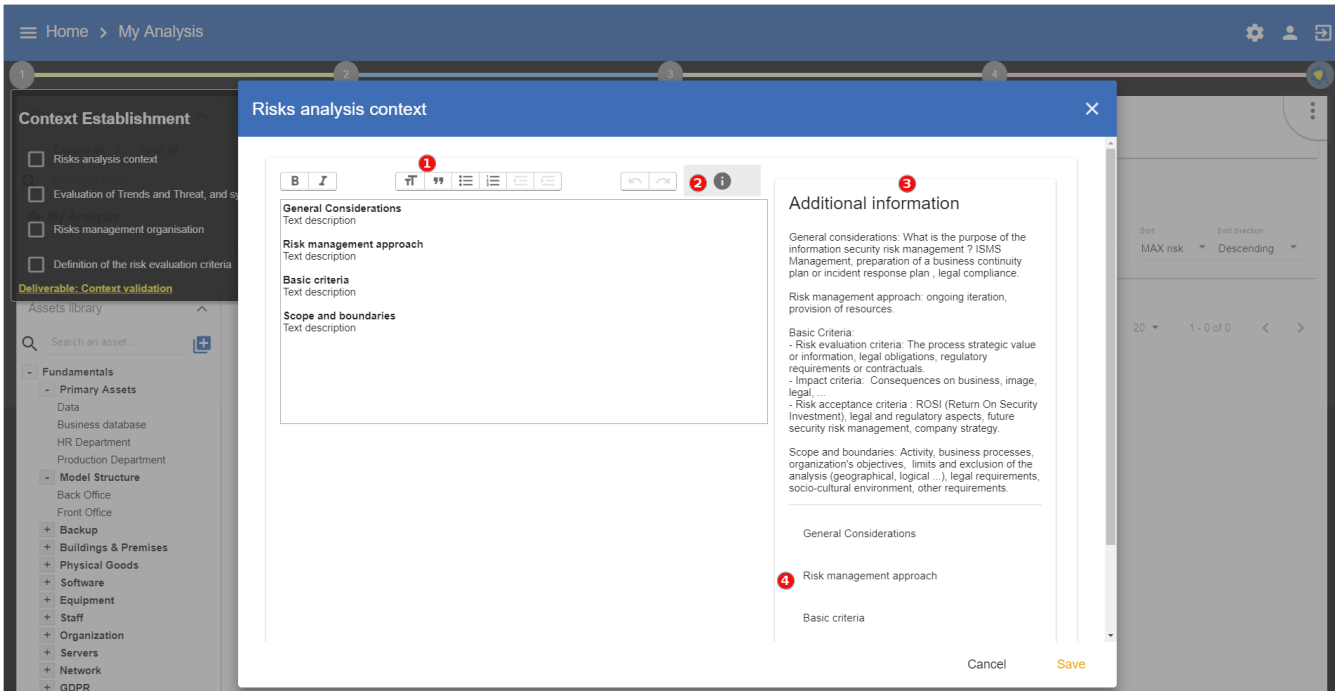
By clicking on number 1, the following menu will appear:



1. Link to the contextual management pop-ups, see the following chapters.
2. Boxes to tick, indicating that the stage selected has closed. This optional information helps to show the progress of the risk analysis project and display the risk representation graph of the dashboard.
3. Link enabling the `Validation of the context` deliverable to be generated. As part of a consultancy assignment, for instance, it may be helpful to get the client to validate it.

3.1. Risk analysis context

This view offers text encoding and formatting functions, enabling the risk analysis target to be contextualised with well-formatted texts that will be documented in the deliverables.

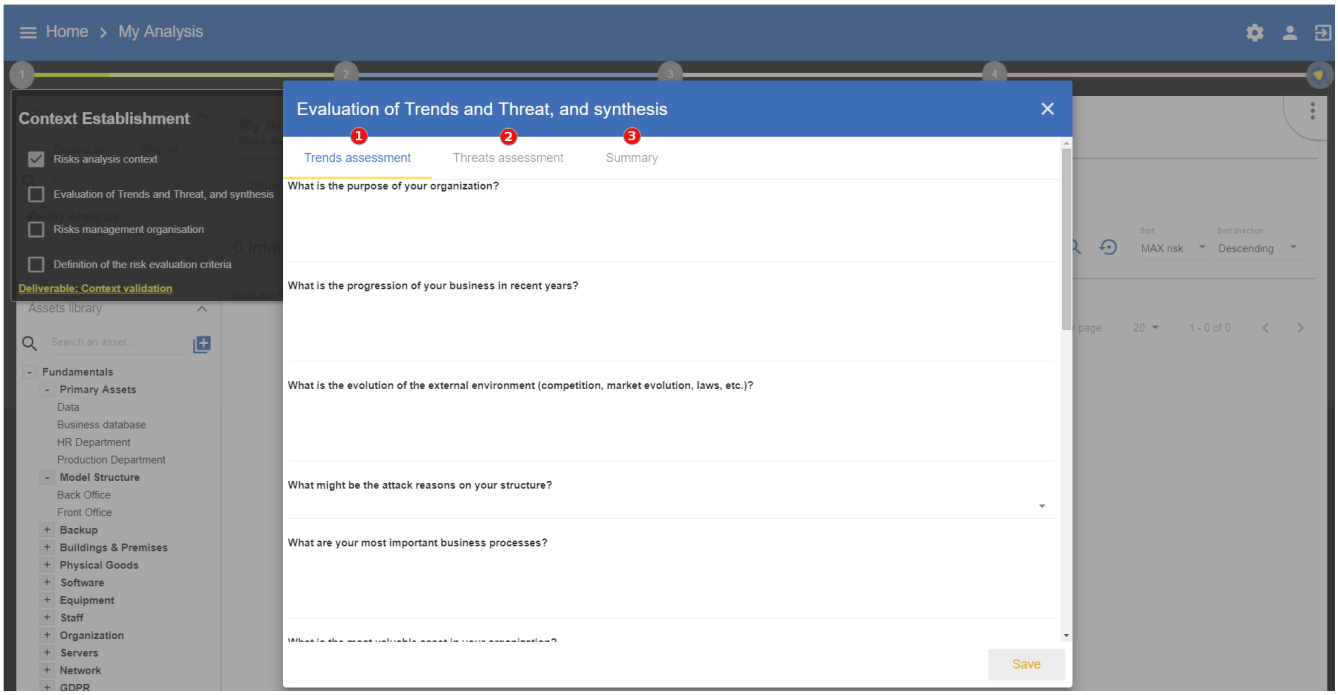


1. Access to the text formatting functions (bold, italics, paragraph, text size, etc.). The quality of the

encoding directly affects that of the deliverable.

2. To display or delete the help area.
3. Help area on the content which is recommended for data entry (`Additional information`).
4. Chapters recommended by ISO27005. Clicking on the label will place it automatically in the data entry area.

3.2. Evaluation of the trends, threats and synthesis



This stage is divided into three separate parts which structures the data collection necessary for understanding the context to analyse. It is advisable to chair a working party of 5 to 10 people (depending on the organisation), bringing together the members of management, IT, risk management department (if it exists), the heads of departments or key personnel.

1. `Trends Assessment`: MONARC provides a series of questions to establish the context from a very general perspective (see Trends Assessment).
2. `Threats Assessment`: Enables the threats to be reviewed from a general viewpoint and, possibly, to evaluate by default in the future model (for more information, see Threats Assessment).
3. `Summary` of key points determined during stages 1 and 2 (for more information, see Summary).

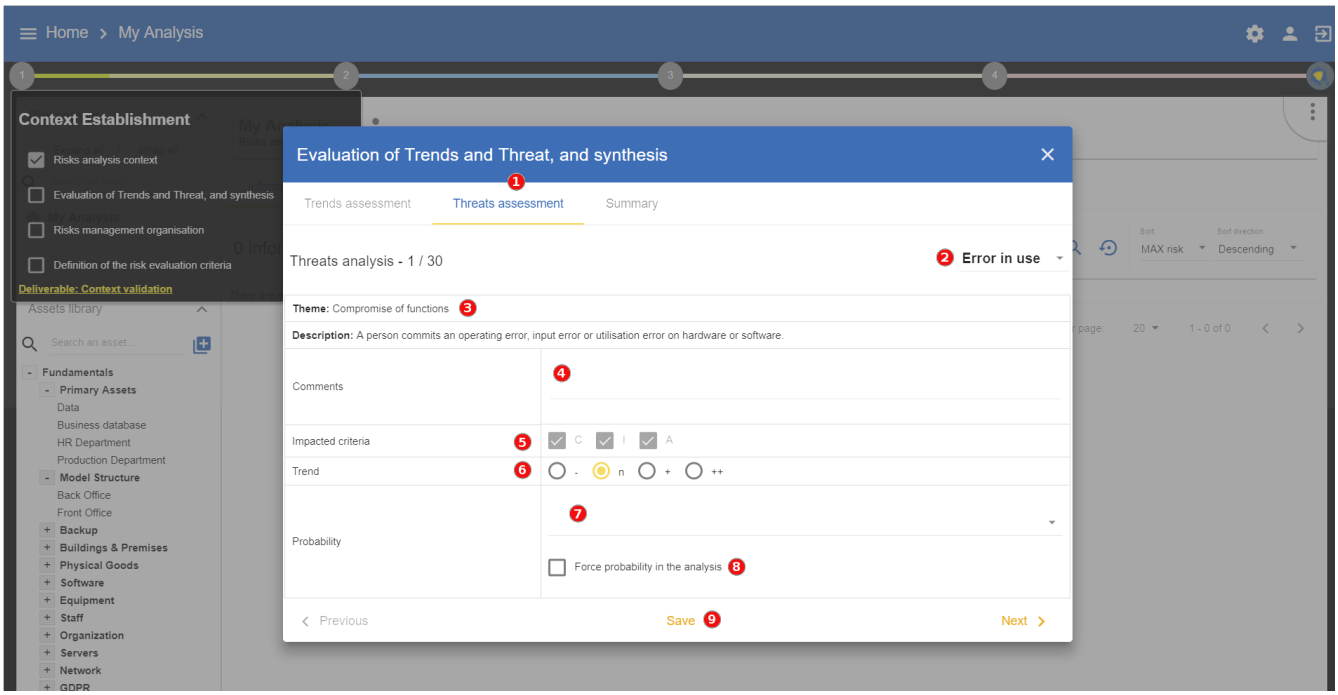
3.2.1. Trends Assessment

The assessment of trends provides a series of questions to establish the context from a very general perspective. These questions highlight the selection of key assets which must be taken into account during the analysis, the security criteria, as well as a few indicators concerning the motives of the attack and the external context of the target. This list is not exhaustive; you can add questions of your choice at the end of the page.

3.2.2. Threats Assessment

The assessment of threats, in similar fashion to the assessment of trends, takes the form of a meeting involving key personnel in the organisation. The purpose is to review the majority of threats by gathering information on the past and reviewing the general observations made by the group. The principle is to obtain a consensus on the probability of the threat on a scale which is easy to interpret:

- Relatively `-`: Never occurred, really not likely
- Normal `n`: No clear position, no opinion
- Relatively `+`: Already occurred
- Relatively `++`: Already occurred on one or two occasions The security expert is responsible for converting the consensus into a probability value of 1 to n which shall be used in the model.

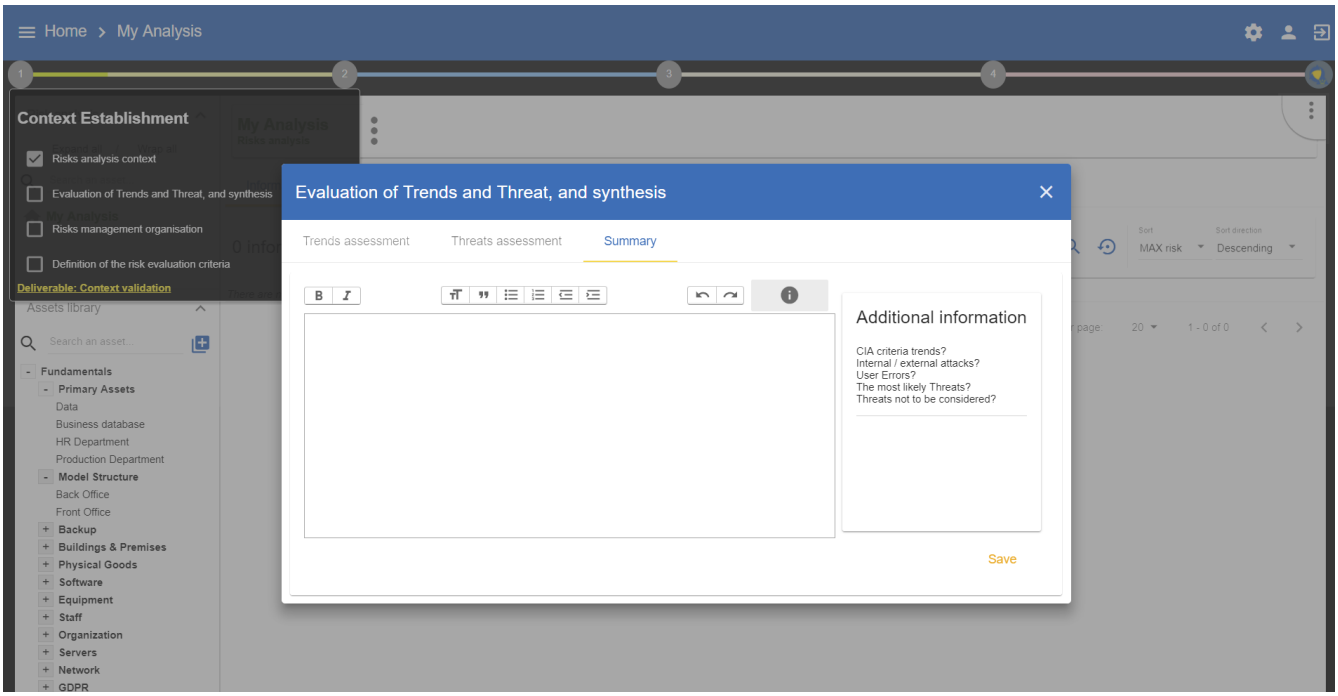


1. Click on the `Threats assessment` tab.
2. Heading of the threat.
3. Information on the threat.
4. Observation to encode, information gathering from a group of persons.
5. Information on the security criteria affected by the threat.
6. Choice of the trend, obtained by group consensus.
7. Selection of the probability deduced from point 6 by the security expert.
8. Possibility of subsequently running the threats of the model (after they have been developed).
9. `Save` the information and browse the threats.

For point 7 and 8, you have to set the scales of your risk analysis to unhide this funtion (see Definition of the risk evaluation criteria)

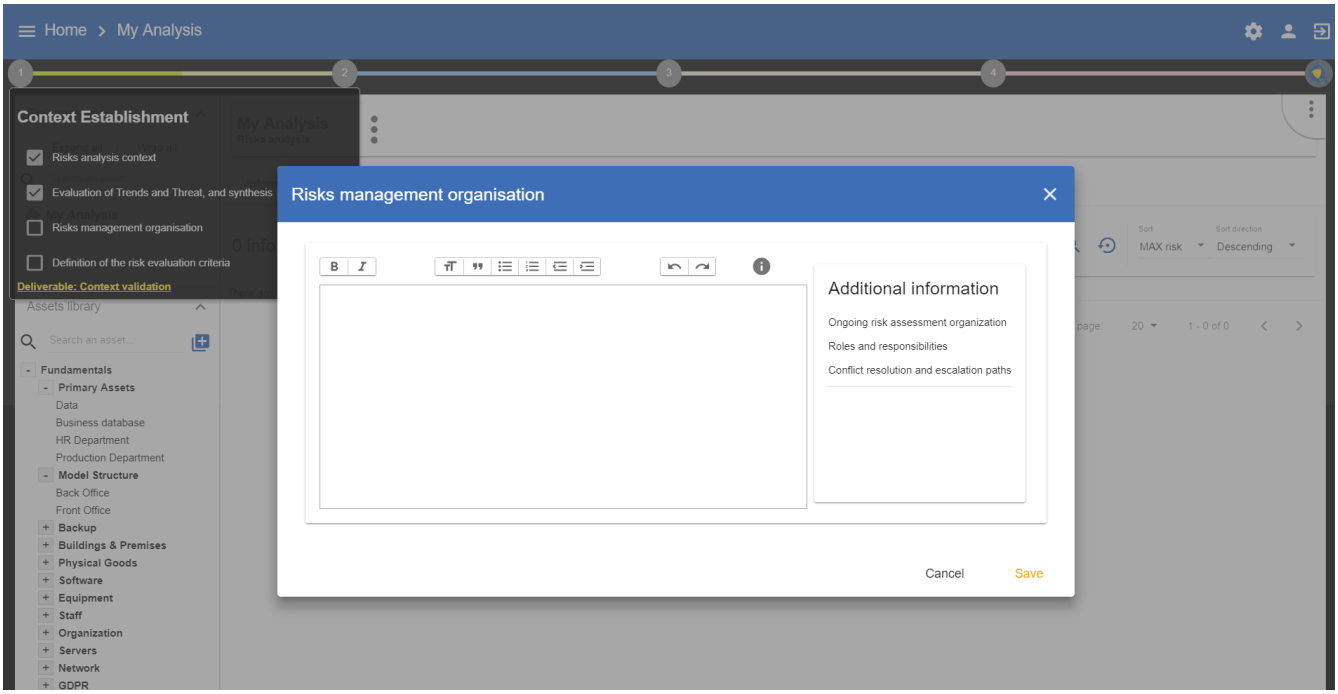
3.2.3. Summary

In similar fashion to the context of the risk analysis, this view enables the user to summarise the pertinent information gathered during the assessment of trends and threats. This text enables the user to enrich the deliverable.



3.3. Risks management organisation

This view enables the user to encode the information on the context of the risk management, for instance, with regard to the roles and responsibilities, the stakeholders, etc.

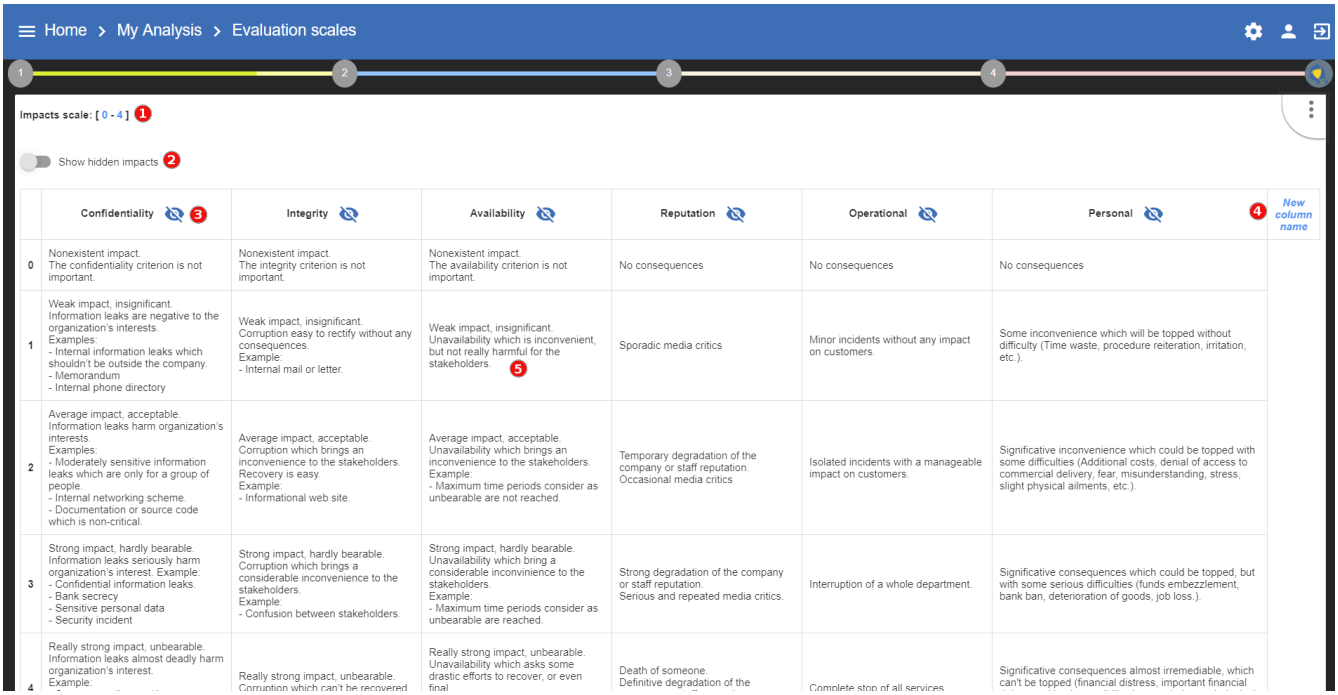


For more information, please see chapter 7.4, of ISO/IEC 27005:2011

3.4. Definition of the risk evaluation criteria

This involves personalising the scales and impact criteria and consequences. MONARC provides values by default which can be personalised depending on the context. All the scales can be modified and the levels personalised. However, it is no longer possible to modify the scales when an assessment has been encoded.

3.4.1. Impact scale



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

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

the management is similar to an Excel table, by clicking on a heading, it is possible to edit it; clicking on another, the first heading will save automatically and so forth.

By default, the impact and consequence scale includes the following criteria:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability
- **R**eputation
- **O**peration
- **L**egal

- **F**inancial
- **P**erson (impact on the person)

It is also possible to add personalised consequences as well as impact criteria.

The same scales are used to process information risk and operational risk; there is simply a difference of interpretation :

- The information risks are evaluated on the CIA [1: Confidentiality, Integrity and Availability.] criteria by taking into account the ROLFP [2: Reputation, Operational, Legal, Financial and Personal] consequences.
- Operational risks are directly evaluated on the ROLFP [2: Reputation, Operational, Legal, Financial and Personal] criteria

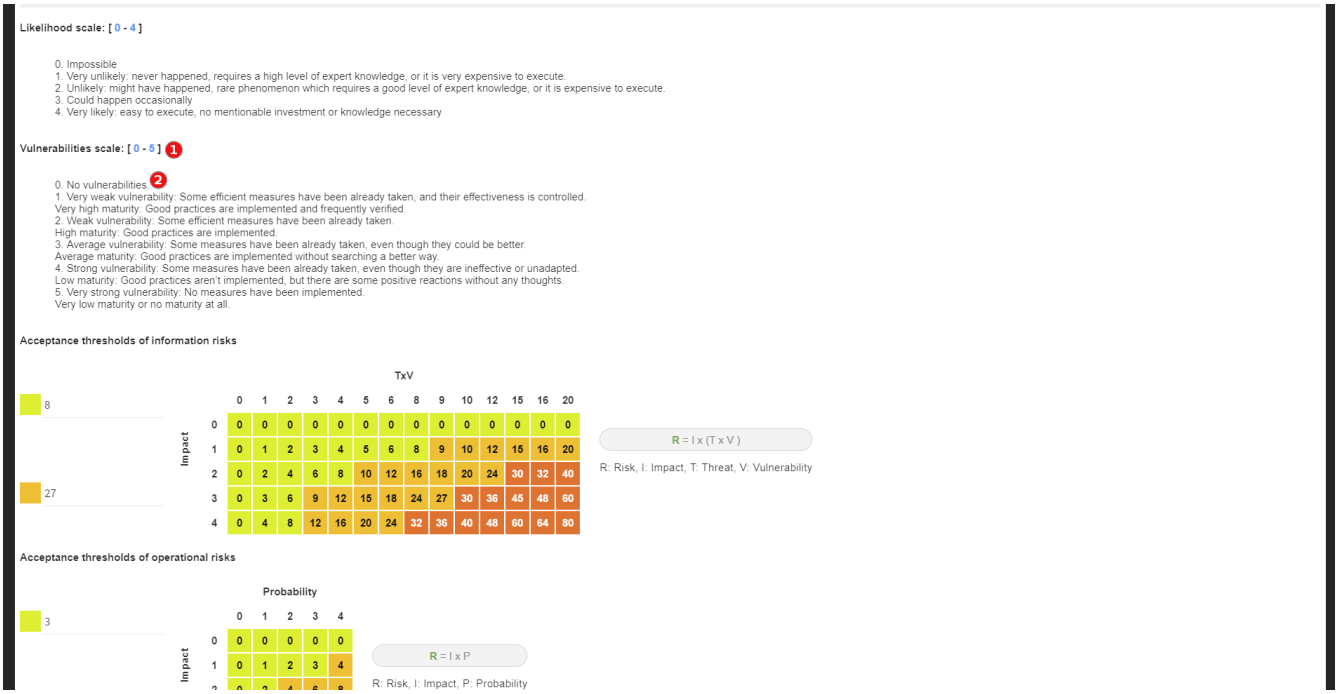
3.4.2. Likelihood scale

The scale of threats is used to calculate information risks and the probability of scenarios relating to operational risks

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

3.4.3. Vulnerabilities scale

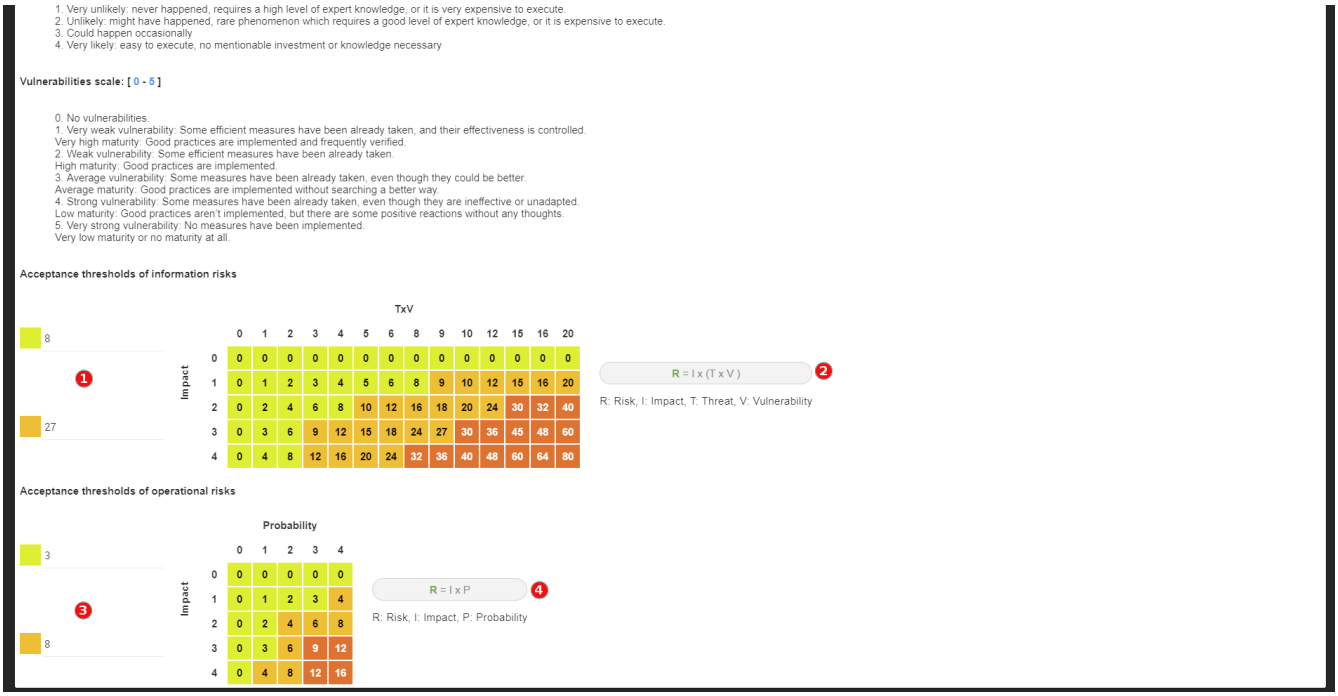
The scale of vulnerabilities is only used for calculating information risks.



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

3.4.4. Acceptance thresholds

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

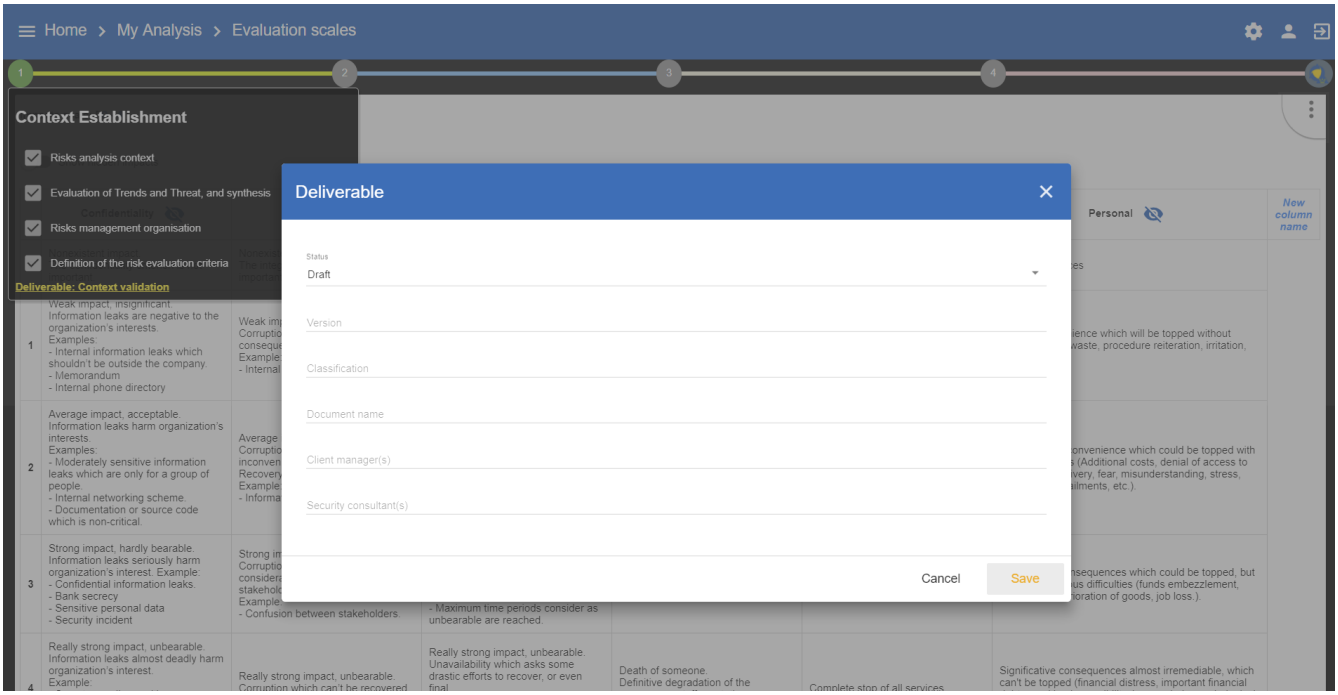


1. Modification of thresholds levels of informations risks. The table displayed above (as well as the risk analysis tables) is updated automatically.
2. Information risks are calculated using three criteria: `Impact x Threat x Vulnerability`
3. Modification of thresholds levels of operational risks. The table displayed above (as well as the risk analysis tables) is updated automatically.

4. Operational riks are calculated using two criteria: `Impact x Probability`

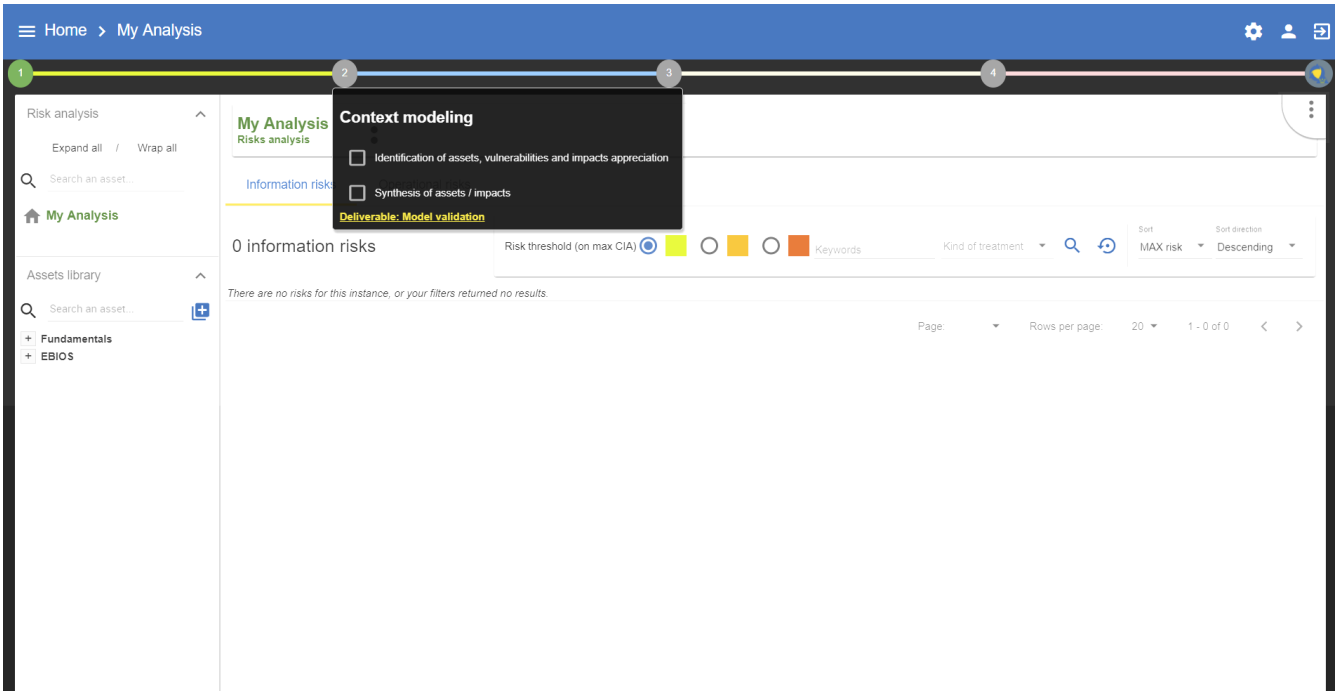
3.5. Deliverable: Context validation

This deliverable includes all the information gathered and entered in the context establishment phase. It can be used to validate the information provided by the client, before beginning the risk identification. A form has to be filled in. When the user clicks on Save, a file in Word format is generated.



4. Context Modeling

By clicking on number 2, the following menu will appear:

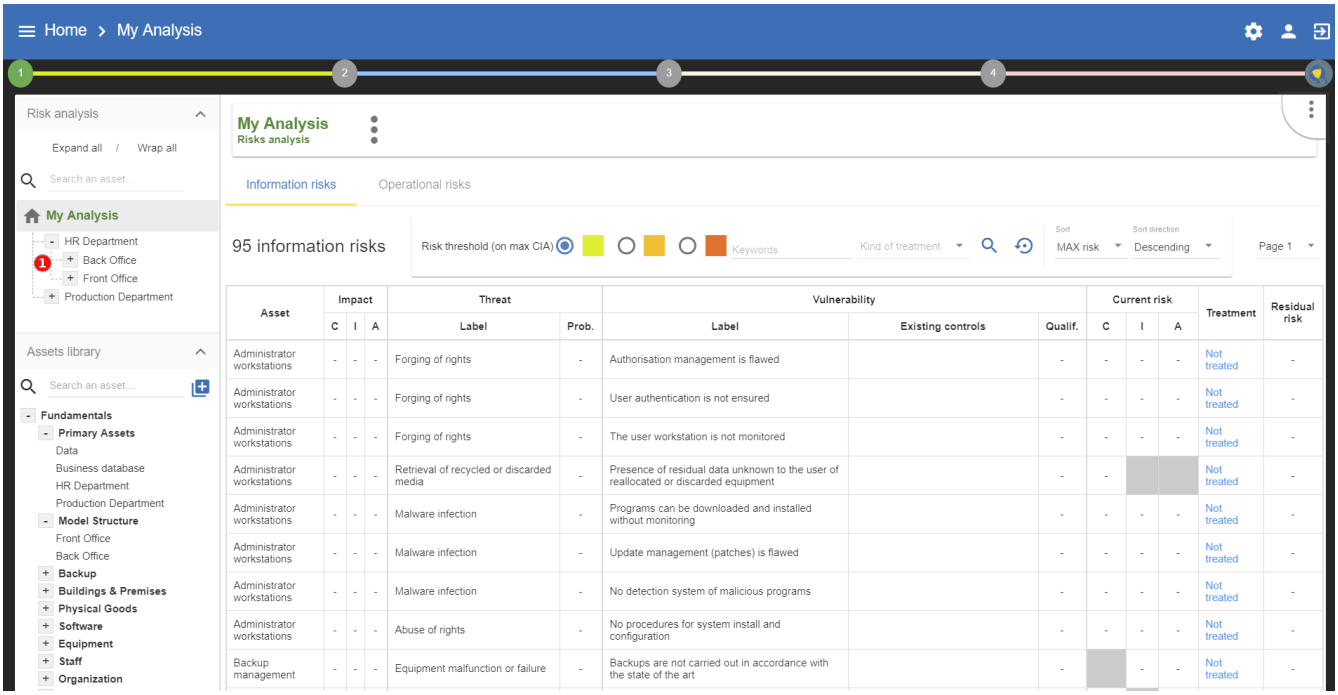


4.1. Identification of assets, vulnerabilities and impacts appreciation

4.1.1. Identification of assets

Clicking on the link `Identification of assets, vulnerabilities and impacts appreciation` will generate the main view of MONARC. The purpose is to create the risk model by using the assets in the library. The principle of the modelling is to place at the root the analysis of the primary assets, then place the support assets which make up the parts above it. The context establishment phase is used for determining the primary assets which will be the subject of the analysis. At this stage of the analysis, certain secondary assets may already be known. By default, MONARC offers a `Front Office` and `Back Office` structure; however, this is not an obligation. It is vital that the construction of the model follows a contextual logic, the assets and terms listed must use the organisation's terminology. To do this, the user must not hesitate to rename the assets provided by default by the library.

Principe of the *front office/back office* structure

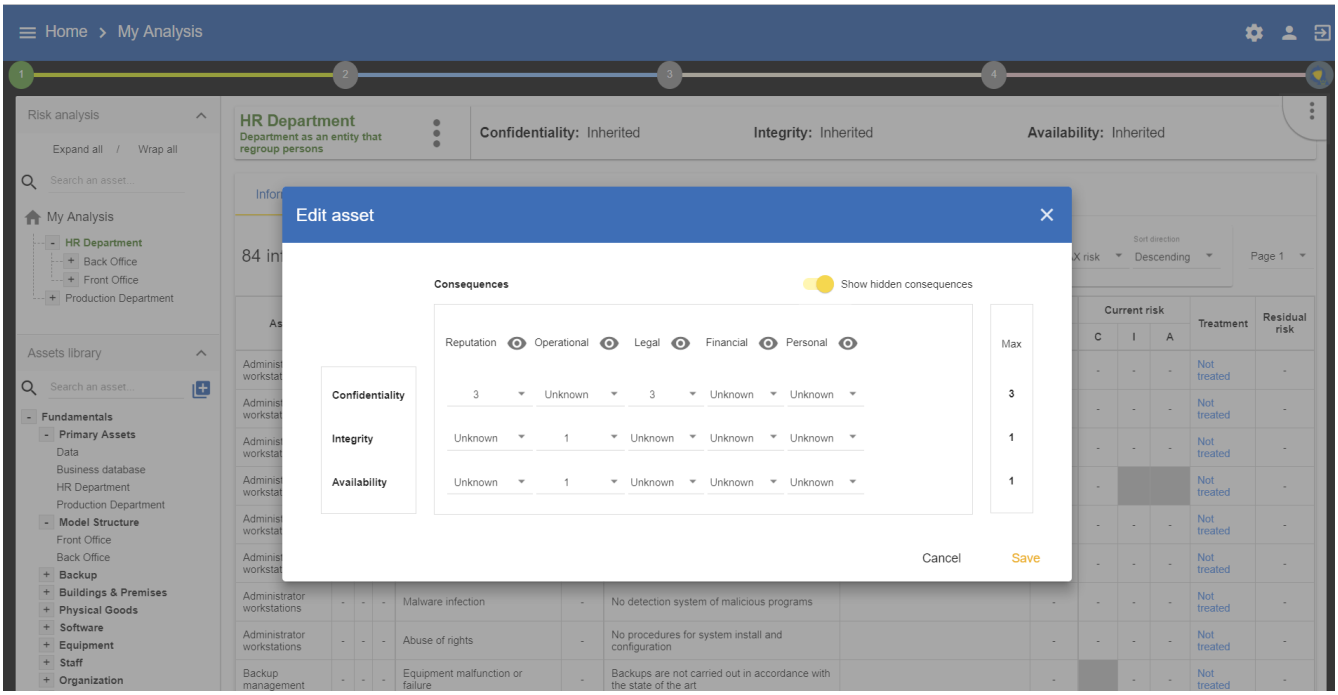


1. The `Front Office` represents the "user" side; for example, in the case of a "Human Resources" department we will find employees and the complete IT system to which they have access (office, workstation, hardware, software, individuals, etc.).
   The `Back Office` represents the IT and organisational side of the organisation that are common to all concerned (building, data centre, network, administrators, common rules, etc.).

4.1.2. Impacts appreciation

For each primary asset, the impact and consequences which may apply must be defined, if the risks in the model arise. By default, all the supporting assets will inherit these impacts, but it is also possible to redefine them. When the primary asset is a service, then the **C** (`Confidentiality`) and the **I** (`Integrity`) refers to the most sensitive information of the service in question. **A** (`Availability`)

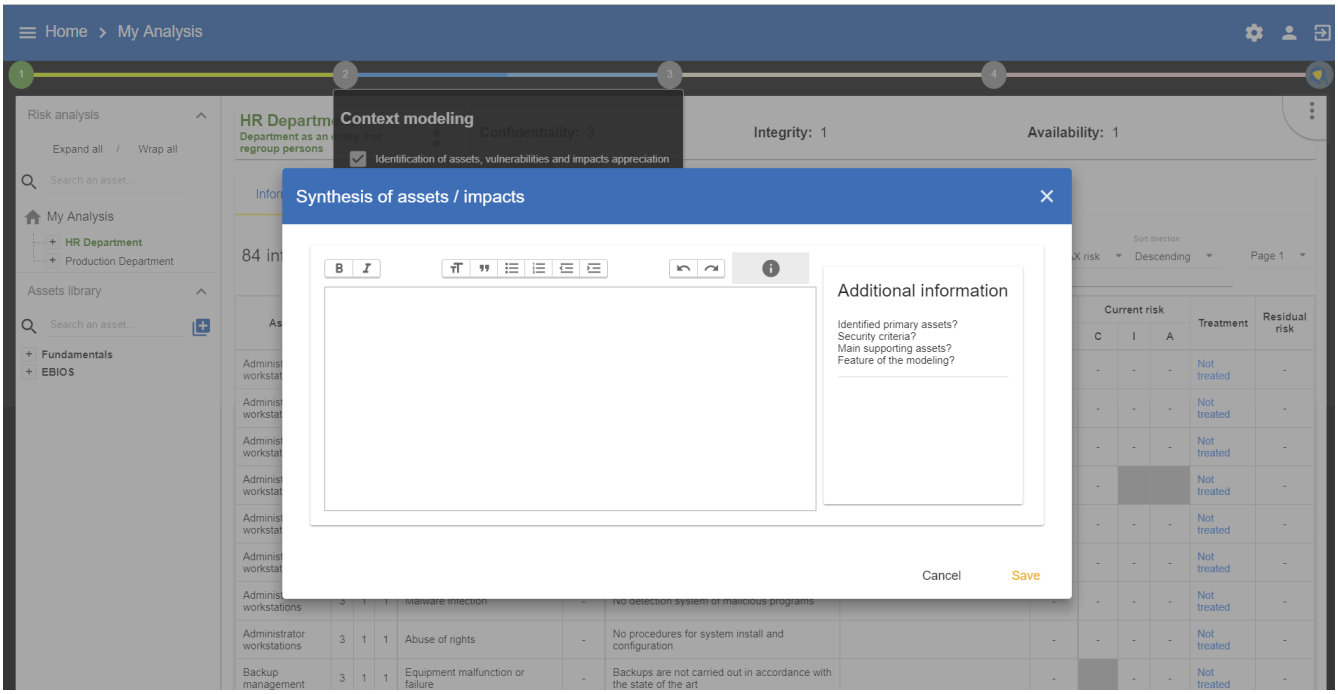
refers to the service and the information, based on the principle that if the information is available, the service will also be available. When the primary asset is the information, there is no ambiguity regarding the CIA criteria - it refers to all the information. In certain rarer cases, if the **C** associated with a service conveys the confidentiality of the operating procedure (e.g. manufacturing process), the user just has to express the assets in the model separately in the form of an informational asset and a service.



The value of the CIA criteria is deduced automatically according to the ROLFP consequences or other consequences which have been associated with them (maximum value). For example: In the case of the abovementioned example, the 3 impact level on confidentiality is explained by the maximum ROLFP value regarding the confidentiality, which in this case is 3 in terms of consequence for the person.

4.2. Summary of assets/impact

The summary of the assets will provide editorial content that justifies the choice of assets and impact for the deliverable.

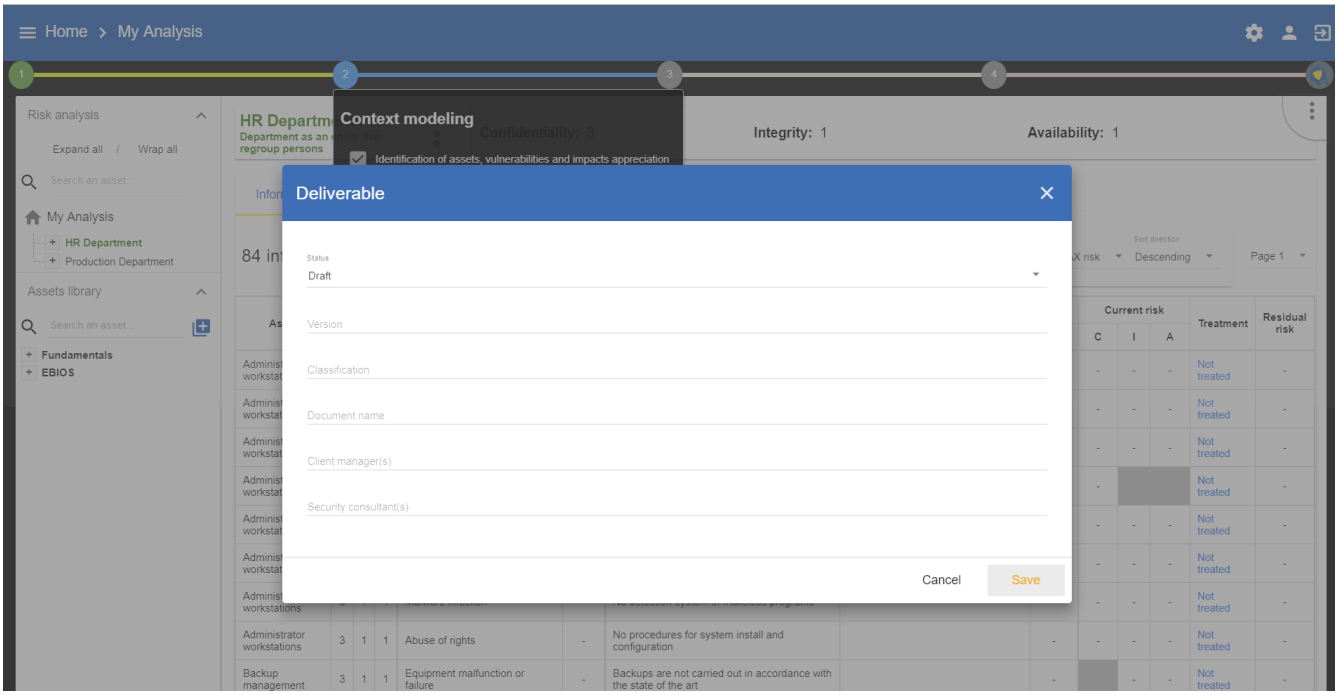


4.3. Deliverable: Validation of the model

This deliverable covers all the significant primary assets of the model.

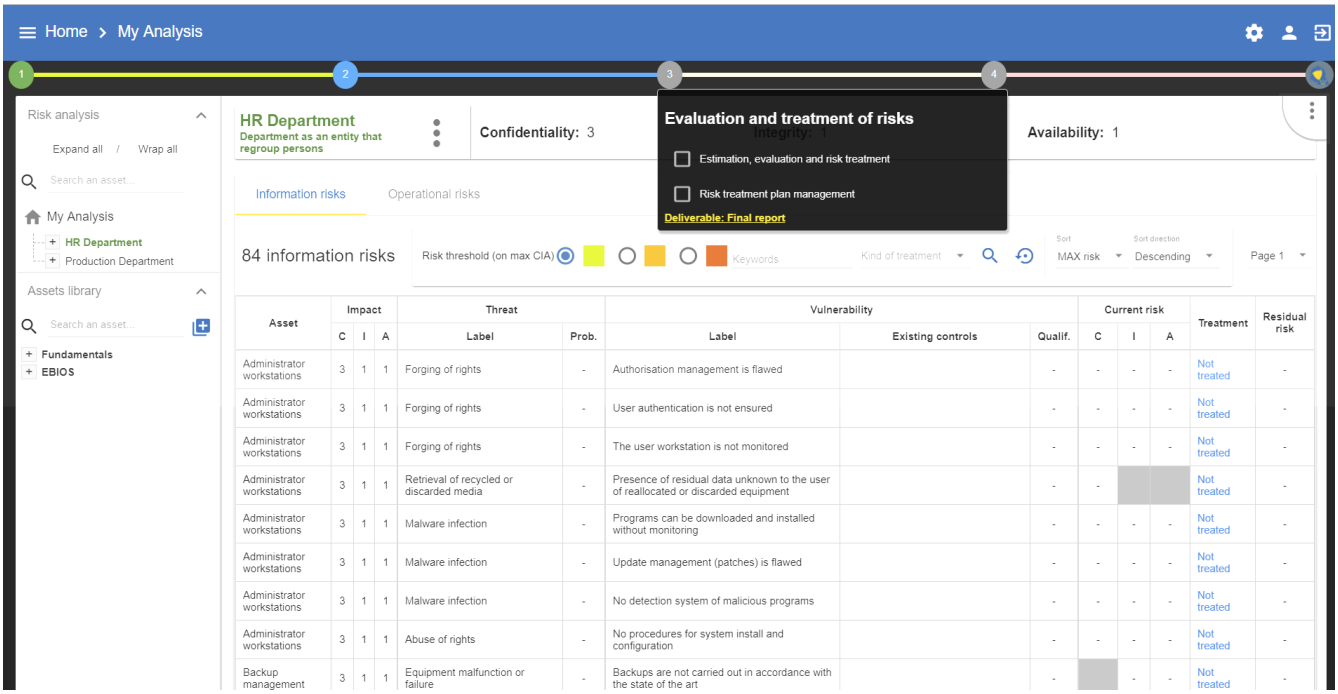
Those on which the impact is reported as well as the asset summary.

A form has to be filled in. When the user clicks on Save, a file in Word format is generated.



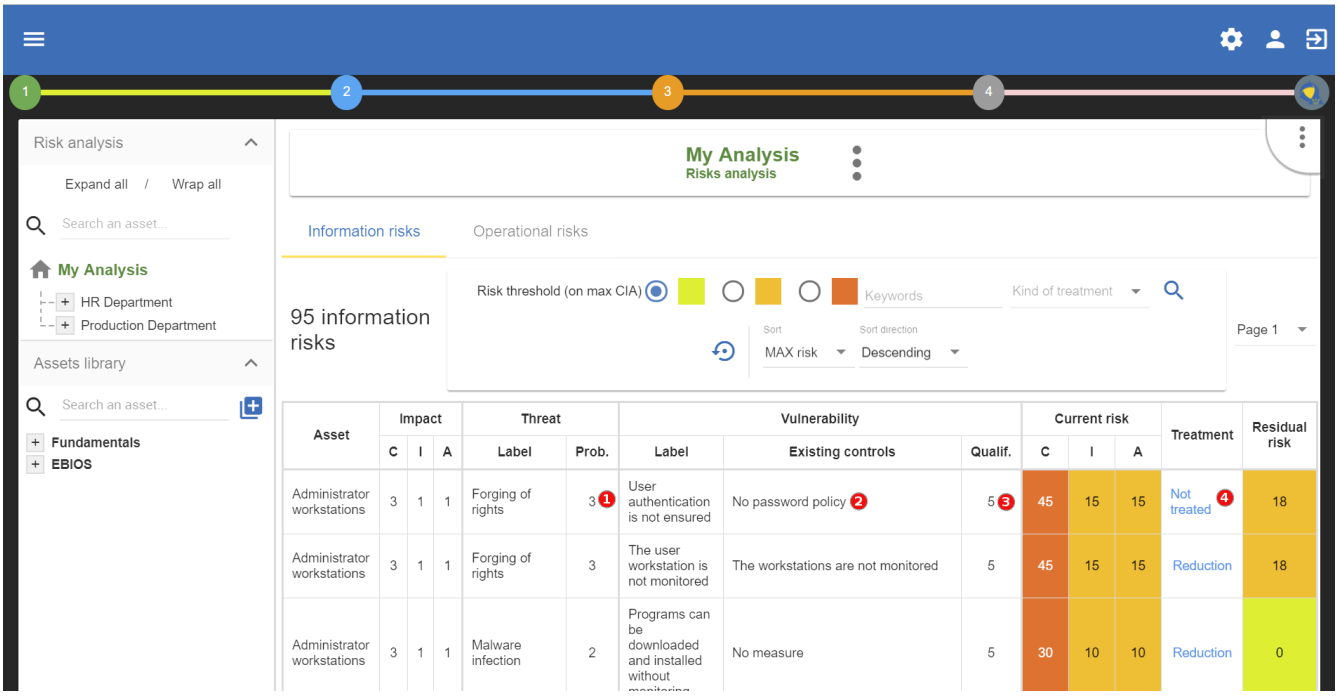
5. Evaluation and treatment of risks

By clicking on number 3, the following menu will appear:



Clicking on the link `Estimation, evaluation and risk treatment` will generate the main view of MONARC.

5.1. Evaluation and treatment of risks



The previous phase provided the impact criteria information; now it is necessary to evaluate threats and vulnerabilities in order to calculate risk levels.

5.1.1. Assessment of the probability of threats

If the threat assessment made while establishing context provided probabilities (see Threats Assessment), it is necessary to return to this screen to run all the threats of the model.

1. `Prob.`: Then, when reviewing the model's risks, the default values may all be revised individually.

5.1.2. Assessment of vulnerabilities

2. The level of vulnerabilities depends directly on the `existing controls`. It is necessary to describe all these measures in a factual manner.
3. The `qualification` of the vulnerability can be set according to the `existing controls`.

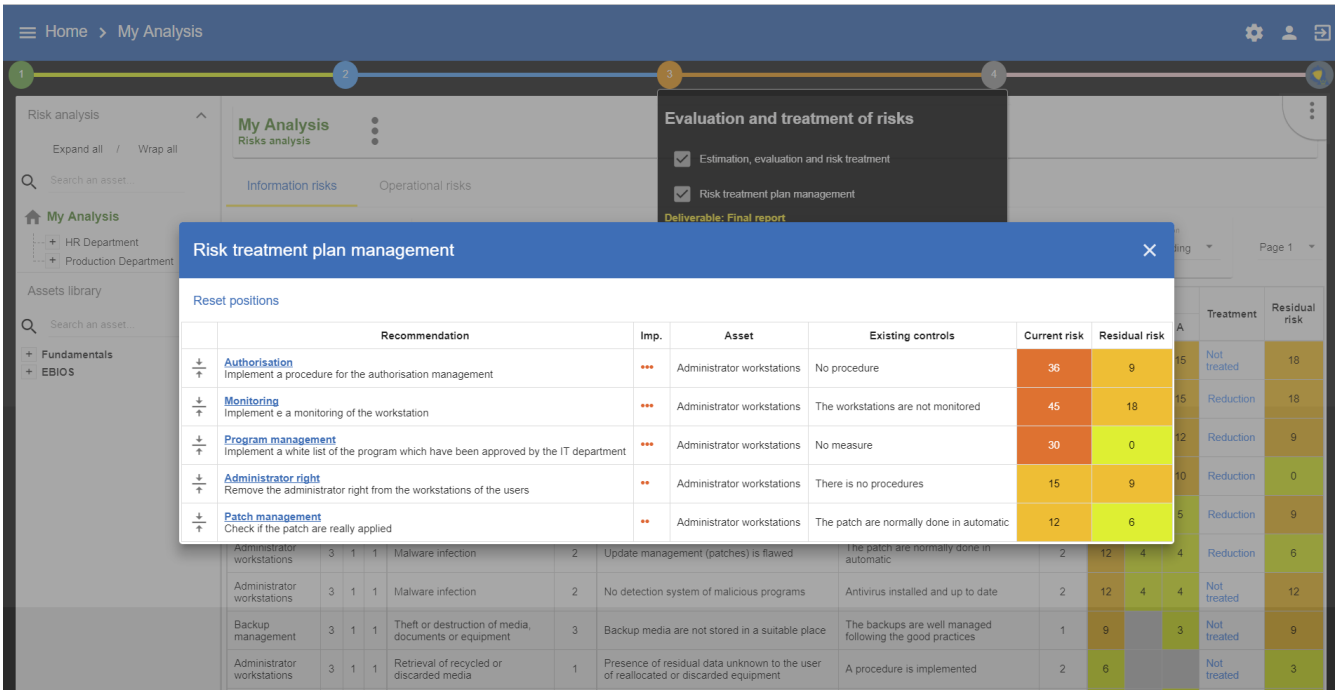
5.1.3. Risk processing

4. Processing risks in MONARC, by clicking on `Not treated`, involves, in similar fashion to ISO/IEC 27005, making a decision so as to process. There are four ways to process the risk:
    - `Accept`: The risk is accepted in its current form. No additional action will be initiated.
    - `Modify/reduce`: Measures are put in place to reduce the risk to an acceptable level. The reduction level is then evaluated in order to calculate the residual risk.
    - `Share`: in the case of insurance, for example. This type of processing is specific, as it tends to reduce the risk impact and not the vulnerability. The residual risk cannot be calculated.
    - `Deny`: The cause of the risk is eliminated; after processing, the risk must not longer be present.

It is also possible to add a recommandation to implement see Risk information sheet in user guide.

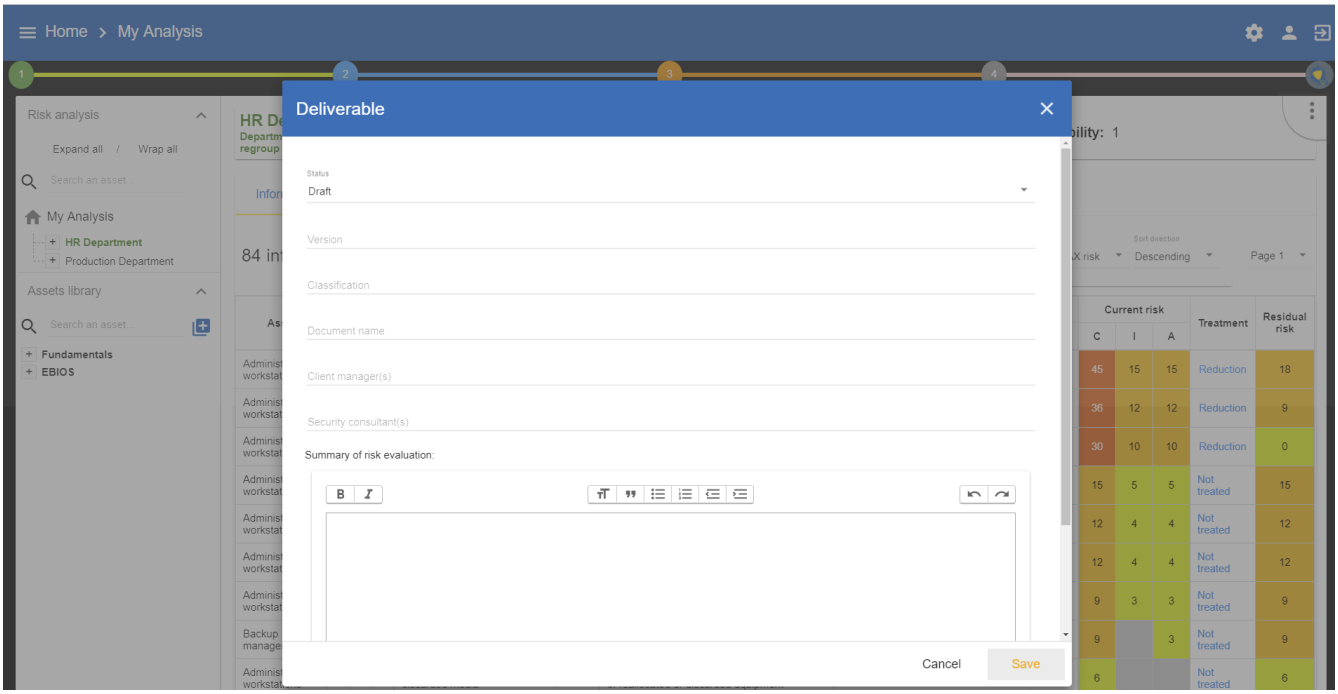
5.2. Risk treatment plan management

All risks covered by one of the four procedures described above are registered in the risk management plan, irrespective of whether they are information risks or operational risks. The calculation formula is not the same for both types of risk; therefore, it is the importance of the recommendations which establish the order of risk. Nevertheless, it is possible to reset the order of the risk processing plan before generating the final deliverable.



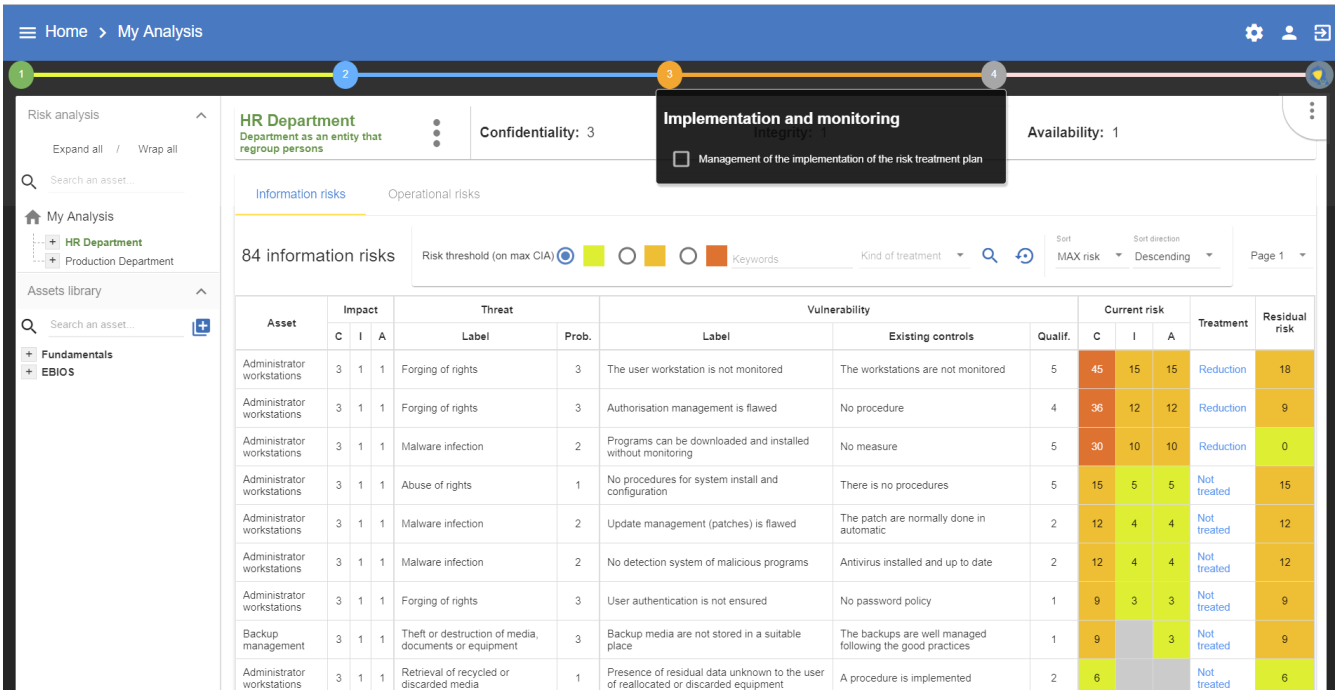
5.3. Deliverable: End report

The deliverable contains a complete list of all the information gathered and entered in MONARC, including that contained in the two previous deliverables. A form has to be filled in. Moreover, it is possible to add a `summary of risk evaluation`. When the user clicks on `Save`, a file in Word format is generated.

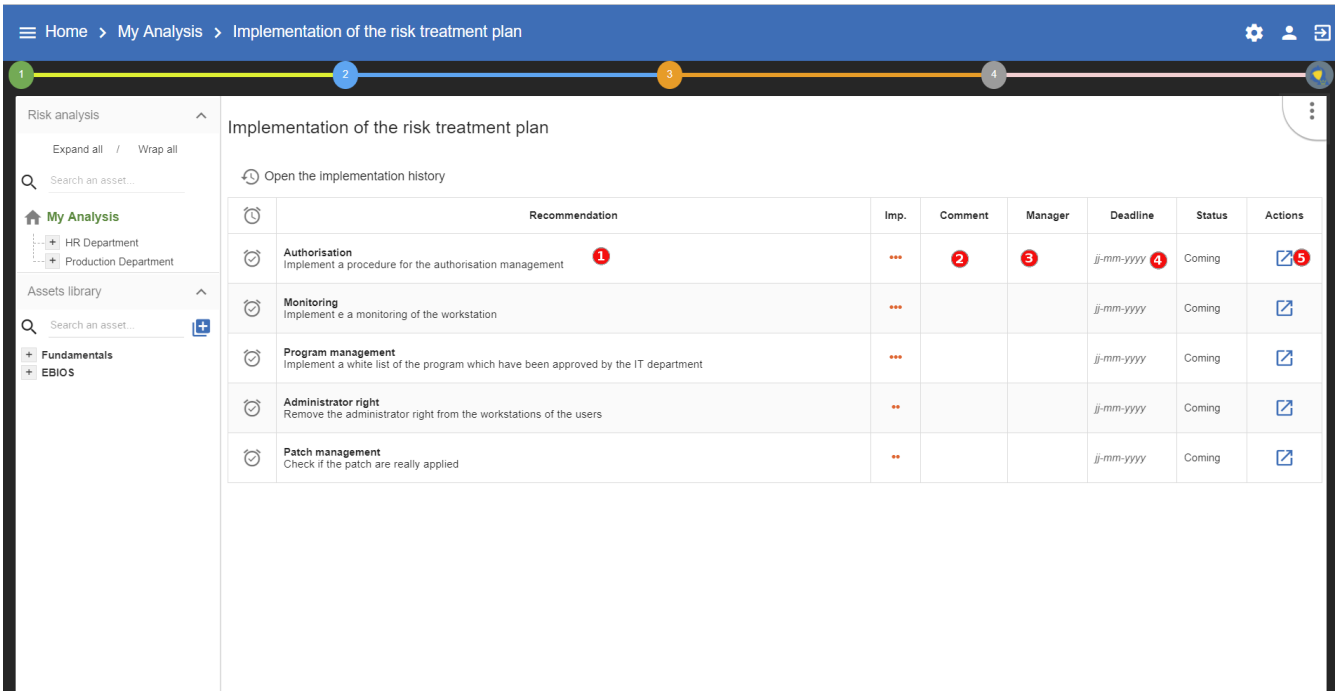


6. Implementation and monitoring

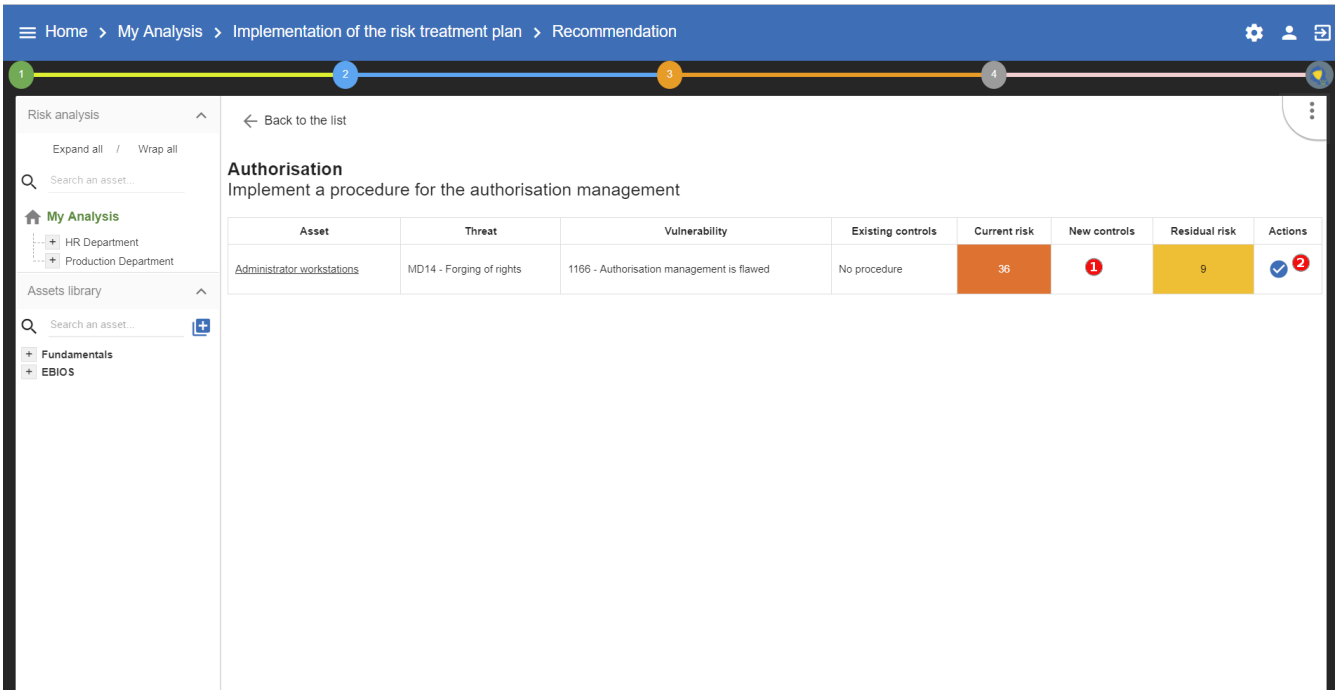
By clicking on number 4, the following menu will appear:



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. You can put a `comment` for the implementation of the recommendation.
3. For each recommendation you can set a `manager`.
4. For each recommenddation you can set a `deadline`.
5. Click on the icon to implement the recommenation and switch on the following view.



1. Set the `new control`, now in place. It will replace the old one in the risk analysis and also replace the old current risk by the residual risk.
2. Definitively validate the measure by clicking on `the icon`.

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