

Method Guide

NC3 Luxembourg

Version 2024-11-25

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	2
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	6
3.1. Risk analysis context	6
3.2. Evaluation of the trends, threats and synthesis	7
3.3. Risks management organisation	10
3.4. Definition of the risk evaluation criteria	10
3.5. Deliverable: Context validation	14
4. Context Modeling	16
4.1. Identification of assets, vulnerabilities and impacts appreciation	16
4.2. Summary of assets/impact	18
4.3. Deliverable: Validation of the model	19
5. Evaluation and treatment of risks	20
5.1. Evaluation and treatment of risks	20
5.2. Risk treatment plan management	21
5.3. Deliverable: End report	22
6. Implementation and monitoring	23
6.1. Implementation history	24
6.2. Deliverable: Implementation Plan	25

Chapter 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](#): Provides a quick start guide about MONARC.
- ¥ [User Guide](#): Provides the complete documentation of the tool.
- ¥ [Technical Guide](#): Provides the complete technical documentation of the tool.

1.3. Syntax used in the document

All numbers displayed in white on an orange background are used in 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

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.

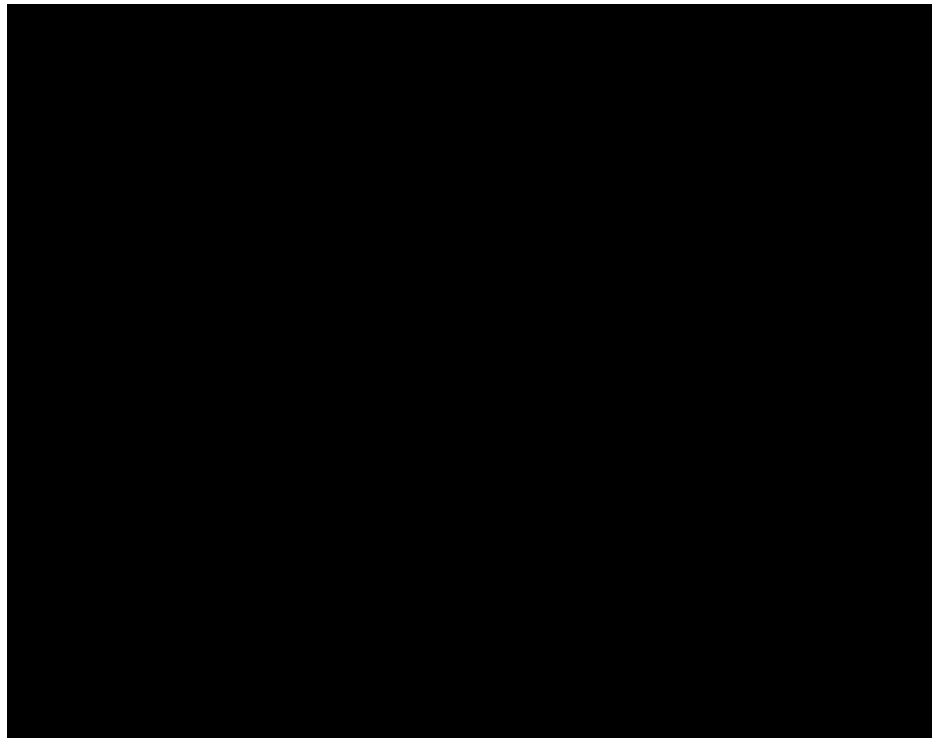
Export any table (.csv) or graphic (.png).

Chapter 2. 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. As recommended by ISO 27005, this method allows the user to focus on the essentials initially and then perform successive iterations to expand or refine the scope, addressing more technical aspects as needed. The tool's optimized risk models, provided as standard, support this type of risk management.



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. Once the primary assets have been identified, they should be broken down into support assets based on priority. The most common assets are available in the MONARC knowledge base, enabling default risk identification. 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 follow-up views in terms of the implementation of recommendations. Monitoring involves regularly reviewing significant changes within the risk analysis context, as well as any major external changes that might necessitate a redesign of the 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 provides an easier framework for understanding non-tangible criteria related to impact and consequences, such as reputation, operational, and legal factors.

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

Chapter 3. Context Establishment

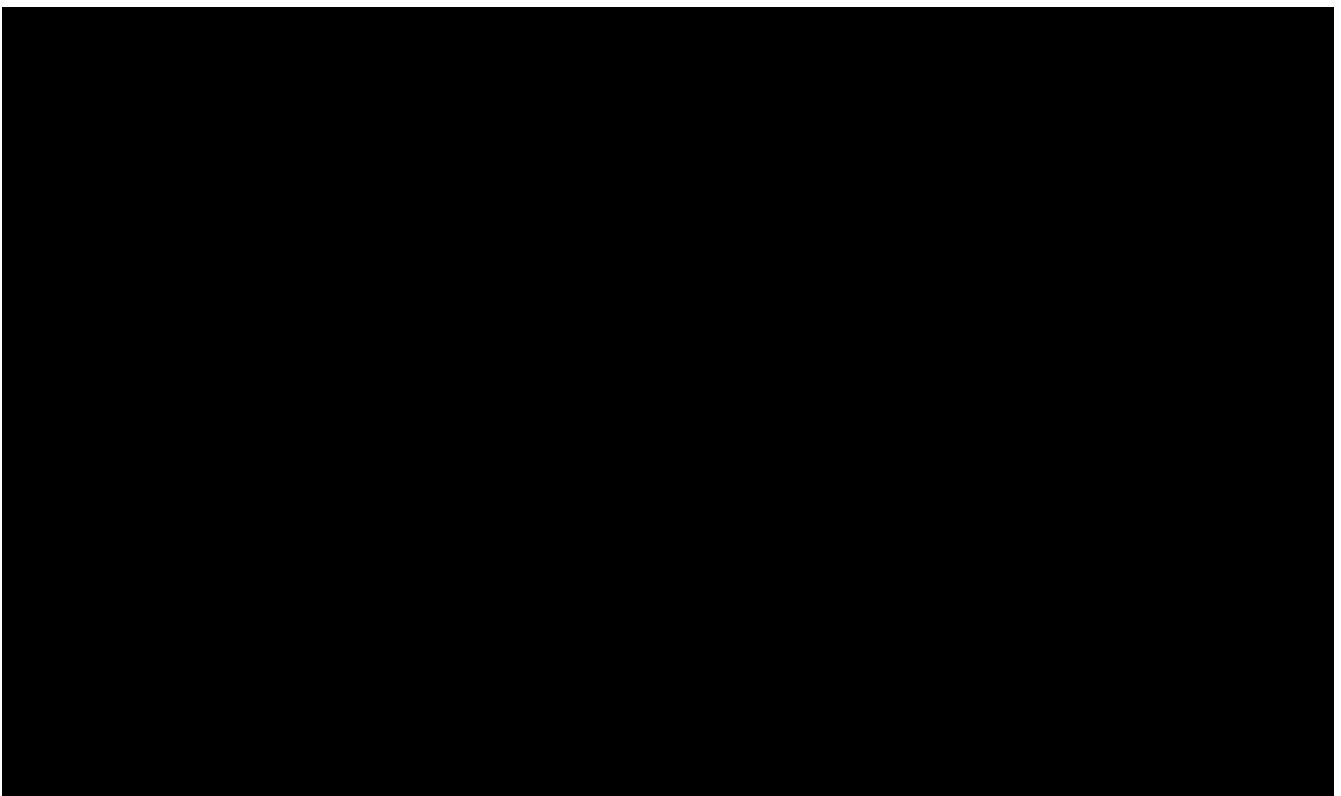
By clicking on number **1**, the following menu appears:



1. Link to the contextual management pop-ups, see the following chapters.
2. Checkboxes indicate that a selected stage has been completed. This feature helps track the progress of the risk analysis project and displays the risk representation graph on the dashboard.
3. A link enables the generation of the context deliverable (Context validation) Validation of the context for validation. As part of a consultancy assignment, for instance, it may be helpful to get the client to validate it.

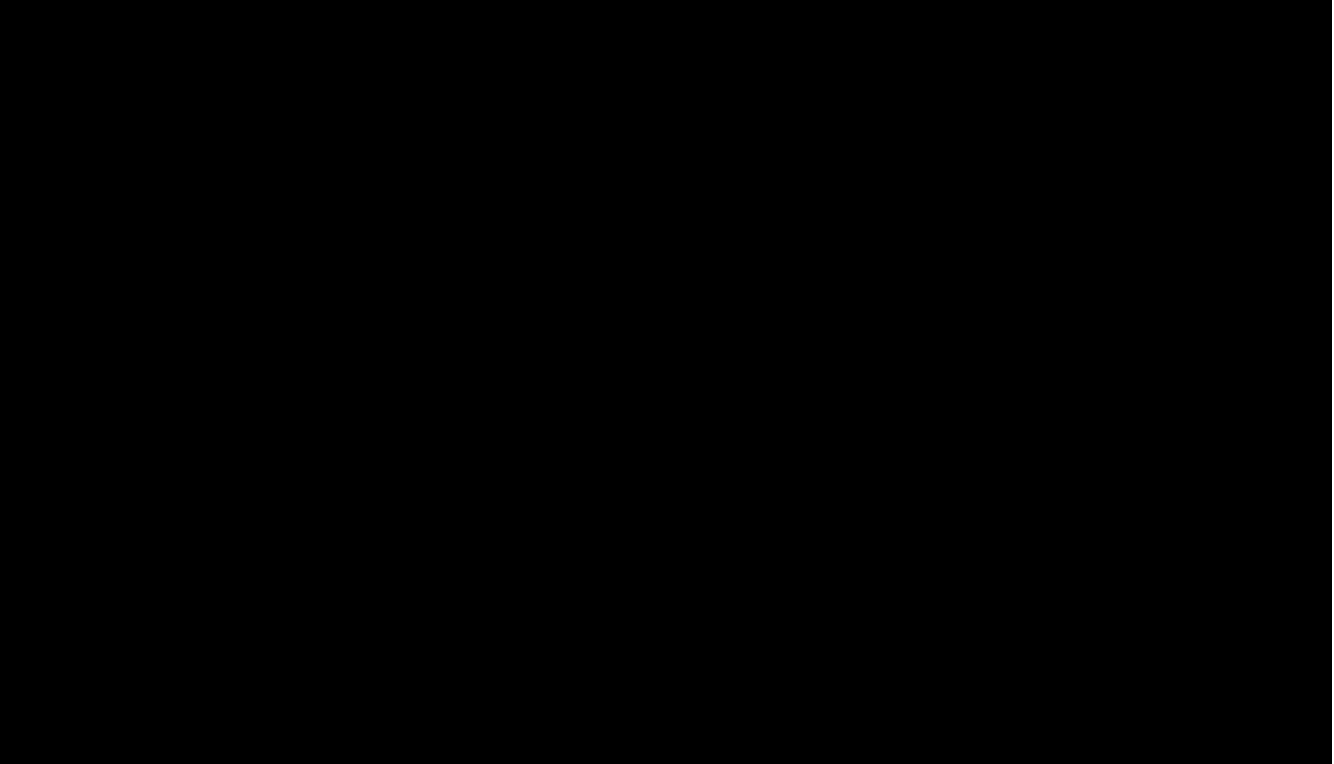
3.1. Risk analysis context

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 has a direct impact on the quality 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 parts to structure the data collection needed for understanding the analysis context. It is recommended to lead a working group of 5 to 10 people (depending on the organization), bringing together management members, IT staff, the risk management department (if applicable), and 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**: It allows threats to be reviewed from a general perspective and, if necessary, to be evaluated 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 a similar fashion to the assessment of trends, takes the form of a meeting involving key personnel in the organisation. The goal is to review the majority of threats by gathering information from the past and examining the general observations made by the group. The objective is to reach a consensus on the likelihood of each threat, using a scale that 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 people.
5. Information on the security criteria affected by the threat.
6. Selection of the trend, determined by group consensus.
7. Selection of the probability deduced from point 6 by the security expert.
8. The option to run the threats in the model later, after they have been developed.
9. **Save** the information and browse the threats.



For points 7 and 8, you have to set the scales of your risk analysis to unhide this function (see [Definition of the risk evaluation criteria](#))

3.2.3. Summary

Similar to the context of the risk analysis, this view allows the user to summarize the relevant 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 in the context of the risk management, for instance, concerning the roles and responsibilities, the stakeholders, etc.

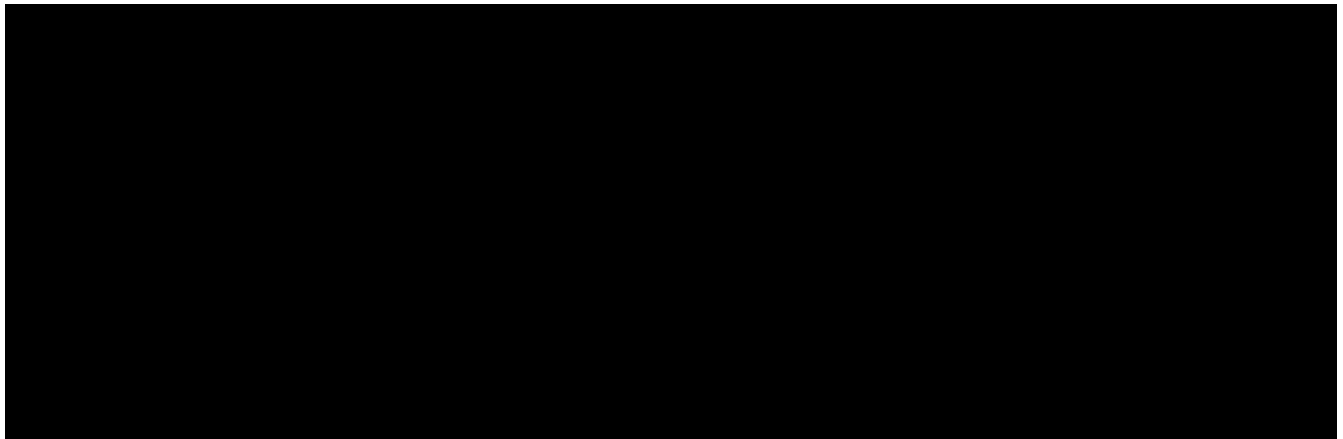


For more information, please see Chapter 7.4, of ISO/IEC 27005:2011

3.4. Definition of the risk evaluation criteria

This involves personalising the scales, 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



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 the **New column name** to add a new impact criteria.
5. Click to edit the headings of each scale.



Managing the headings is similar to working with an Excel table. By clicking on a heading, you can edit it. Clicking on another heading will automatically save the first one, and so on.

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

- ¥ Confidentiality
- ¥ Integrity
- ¥ Availability
- ¥ Reputation
- ¥ Operation
- ¥ Legal
- ¥ Financial
- ¥ Person (impact on the person)

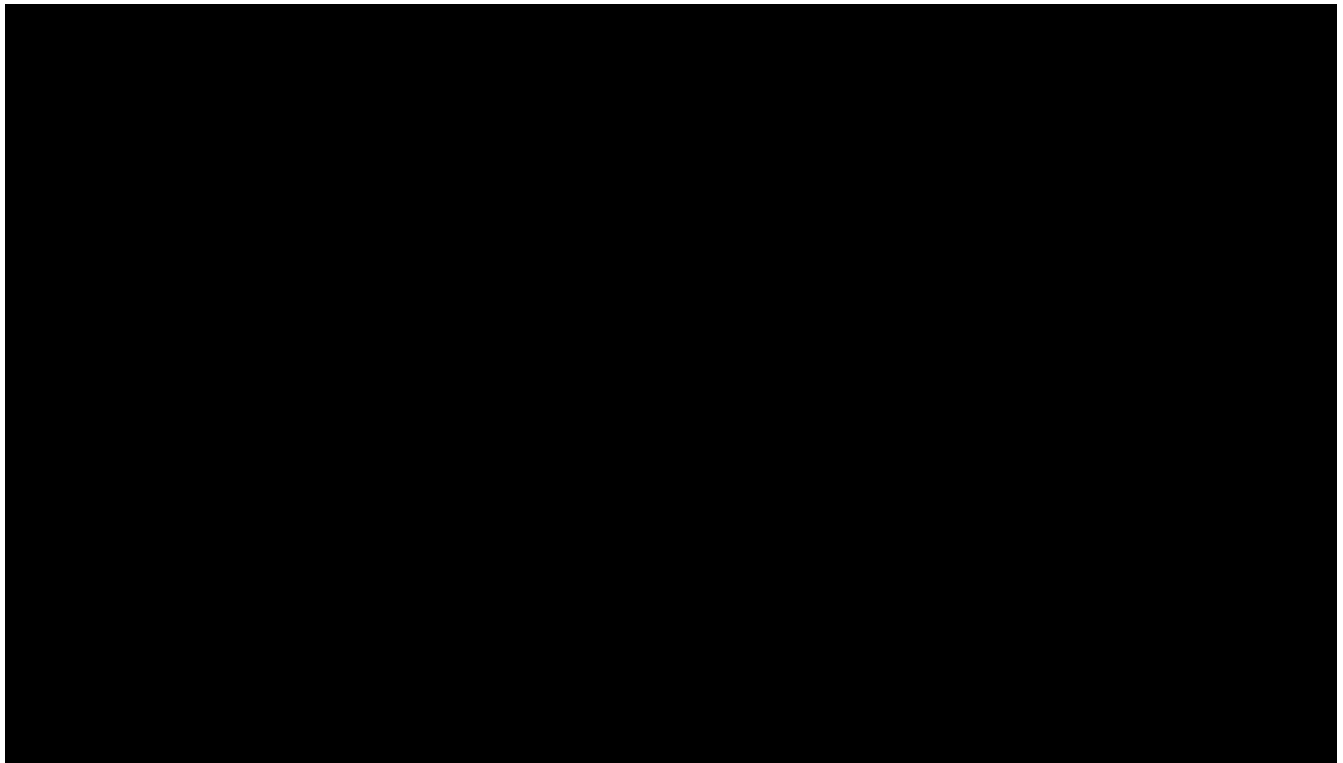
It is also possible to add personalised consequences as well as impact criteria.

The same scales are used to assess both information risk and operational risk; the difference lies in their interpretation:

- ¥ The information risks are evaluated on the CIA^[1] criteria by taking into account the ROLFP^[2] consequences.
- ¥ Operational risks are directly evaluated on the ROLFP^[3] criteria

3.4.2. Likelihood scale

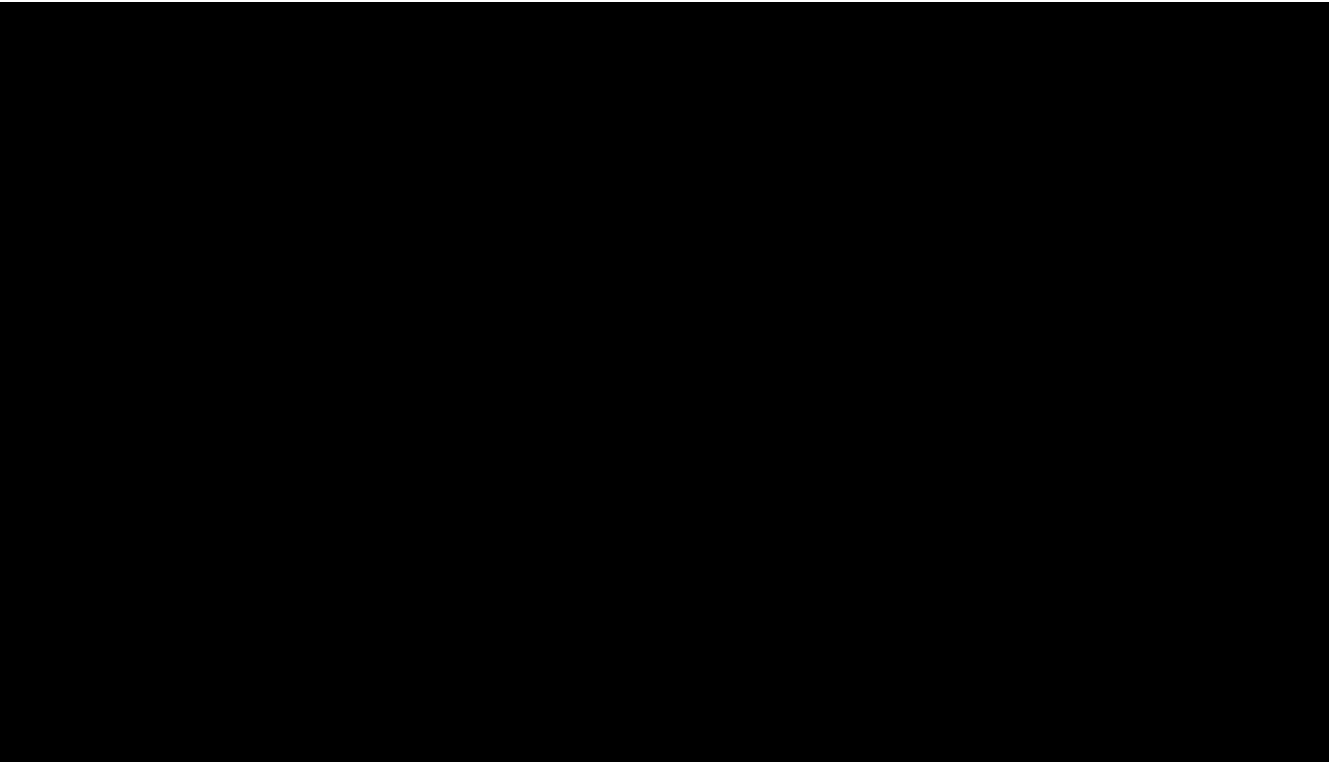
The scale of threats is used to calculate information risks and the probability of scenarios relating to operational risks



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

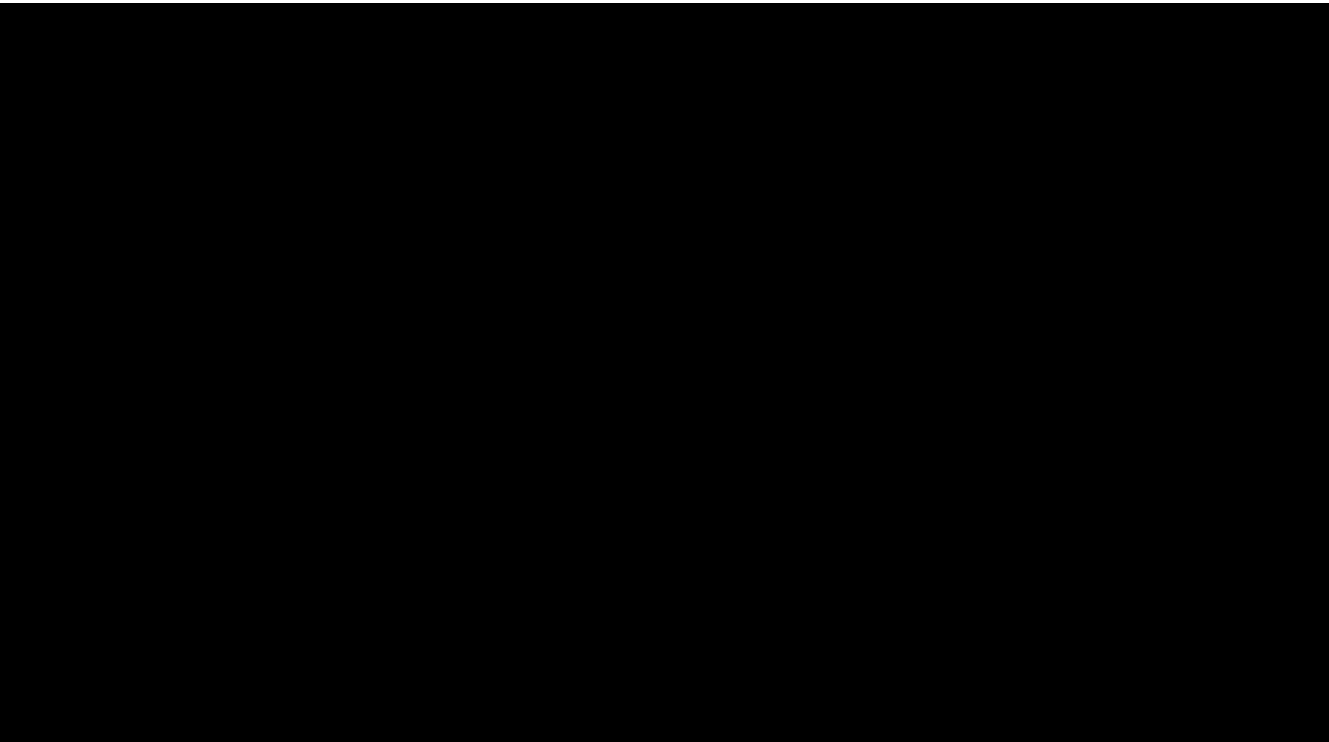
The scale of vulnerabilities is only used for calculating information risks.



- 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 calculated differently. Information risks are calculated using three criteria:



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

3.5. Deliverable: Context validation

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

[1] CIA, Confidentiality, Integrity and Availability.

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

[3] rolfp

Chapter 4. Context Modeling

By clicking on number 2, the following menu appears:

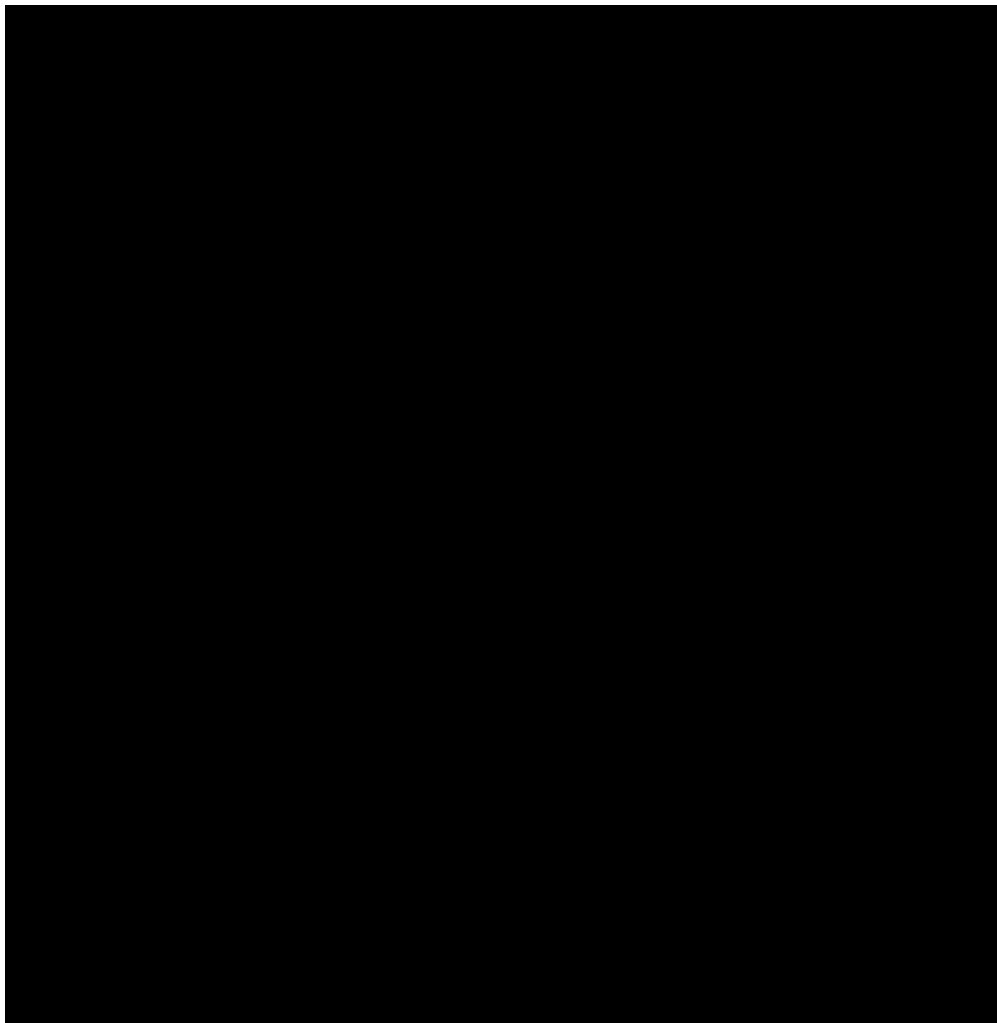
4.1. Identification of assets, vulnerabilities and impacts appreciation

4.1.1. Identification of assets

Clicking on the link [Identification of assets, vulnerabilities and impacts appreciation](#) generates the main view of MONARC. The goal is to create a risk model using assets from the library. The modelling principle involves placing the primary asset analysis at the root, followed by the supporting assets that comprise its components. The context establishment phase is used to determine the primary assets that will be analyzed.

At this stage of the analysis, certain secondary assets may already be identified. By default, MONARC offers a [Front Office](#) and [Back Office](#) structure , although this is optional. The construction of the model must follow a contextual logic, with assets and terms reflecting the organization's specific terminology. To achieve this, users should feel free to rename the default assets provided by the library.

Principe of the *front office/back office* structure



1. The **Front Office** represents the 'user' side; for instance, in a Human Resources department, this includes employees and the full IT system they access, such as office space, workstations, hardware, software, and personnel.
2. The **Back Office**, on the other hand, represents the IT and organizational infrastructure shared across the organization, including facilities like buildings, data centres, networks, administrative roles, and common policies.

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**) refer 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 associated consequences, using the highest applicable value. For example: in the case above, the confidentiality impact level of 3 is set because the highest ROLFP value related to confidentiality is 3, representing the impact on the individual.

4.2. Summary of assets/impact

The summary of the assets provides an explanation that justifies the selection of assets and their impact on 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.

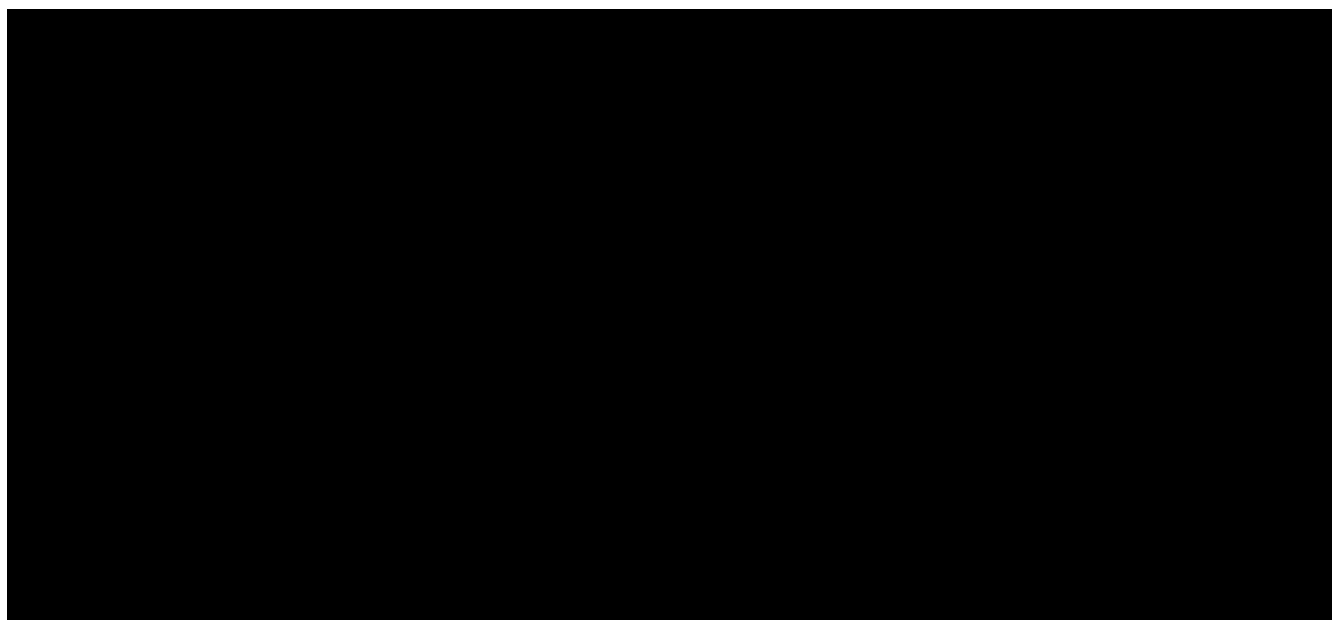
A form has to be filled in. When the user clicks on **Save**, a file in Word format is generated.

Chapter 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 recommendation 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.

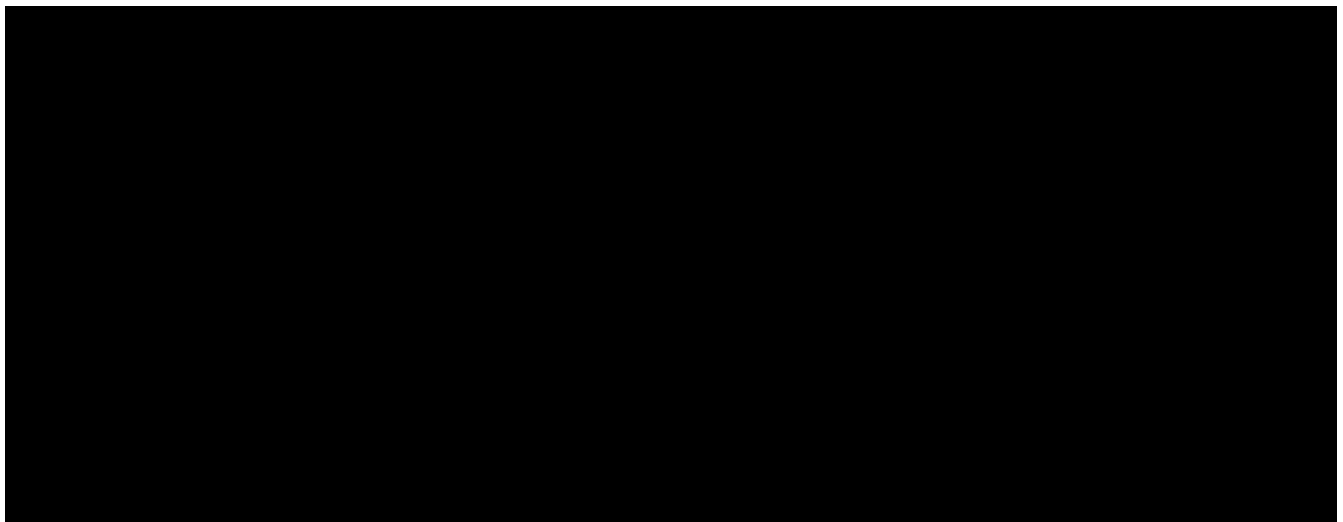
5.3. Deliverable: End report

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.

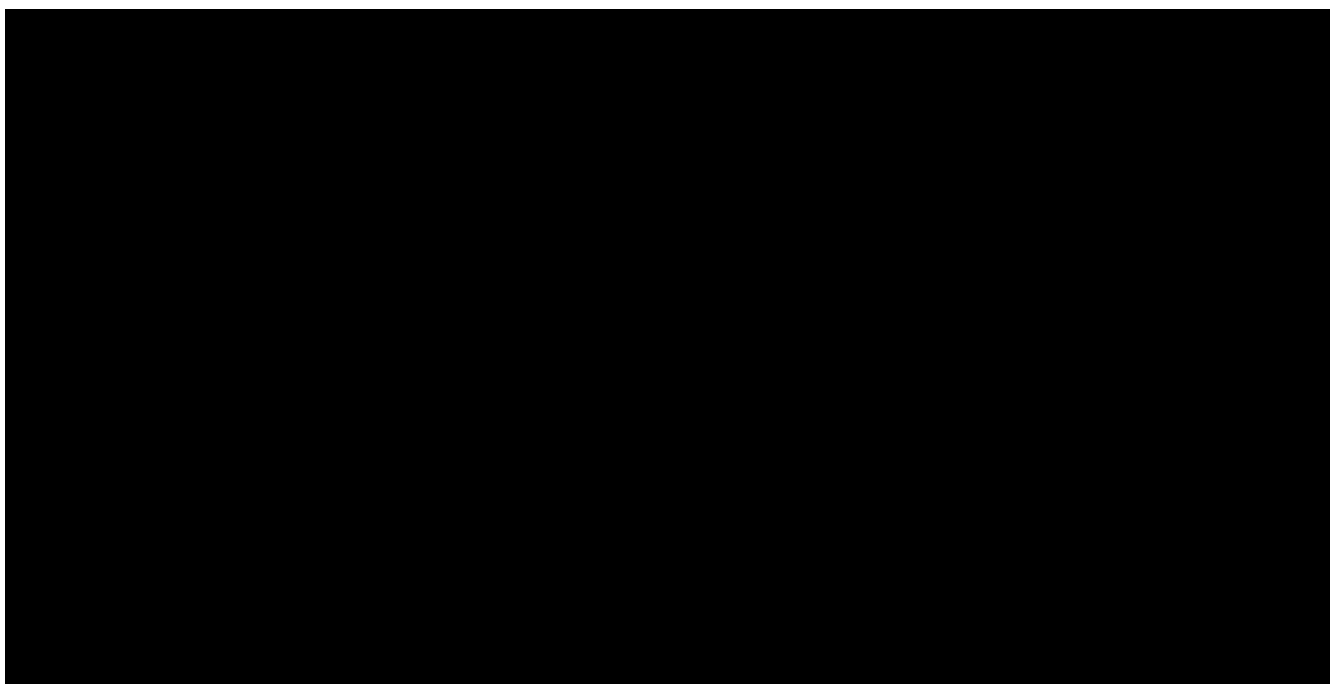
Chapter 6. Implementation and monitoring

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 **recommandati**on established before.
2. You can put a **comment**t for the implementation of the recommendation.
3. For each recommendation you can set a **manager**.
4. For each recommenddation you can set a **deadl i**ne.
5. Click on the icon to implement the recommenation and switch on the following view.



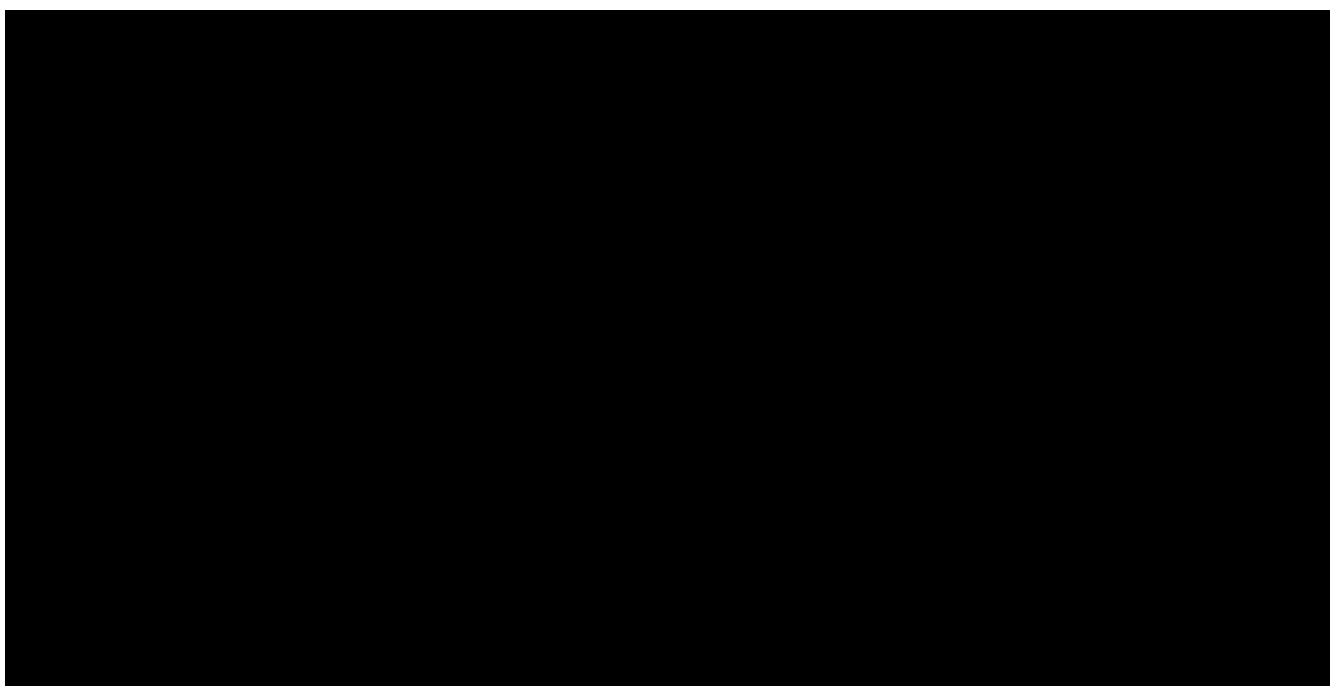
1. Set the **new control**, now in place. It will replace the old one in the risk analysis and also replace the old current risk by the residual risk.
2. Definitively validate the measure by clicking on icon



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

6.1. Implementation history

All validations are stored in history and can be consulted:



1. Click to view past recommendations

6.2. Deliverable: Implementation Plan

The deliverable contains the recommendations to implement table and the implemented recommendations table. A form has to be filled in. When the user clicks on **Save**, a file in Word format is generated.