|  |  |
| --- | --- |
|  |  |
| Organisation name | |
| Title of the project | |
| **Risk assessment and treatment report** | |
|  | |

General information

|  |  |
| --- | --- |
| Sequence number | Q142 |
| Version | 0.5 |
| State | Final version |
| Approved by | …. |
| Date of approval | 07/11/2017 |
| Classification | Internal |

Distribution list

|  |  |  |
| --- | --- | --- |
| Recipient | Channel | Reason |
|  | By email | Validation |
|  | By email | Validation |

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Modifications |
|  | … |  |  |

Working group

|  |  |
| --- | --- |
| Name | Organisation |
| Client’s working group (List with the first letter of surname and name) | Customer |
| itrust’s working group (List with the first letter of surname and name) | itrust consulting |

Approbations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Responsibility | Date | Signature |
|  |  |  | … |  |
|  |  |  | … |  |

Management summary

##### Context

The following document presents the results of the qualitative risk assessment performed by Name of the consultant. This project intended to get a detailed risk assessment and risk treatment plan to increase the security level in the following years. The risk analysis follows ISO/IEC 27005 on risk management and was conducted with the support of the risk assessment and treatment tool TRICK Service developed by itrust consulting.

##### Scope

The scope of the risk analysis consists of summary of the scope

##### Results and limitations

According to the Customer, the results of the present analysis are sufficient to implement the risk treatment and accept the residual risk. However, these results should be refined periodically to describe real state of the risk of the organisation.

##### Risk treatment plan

The risk treatment plan is composed of 0 implementation phases:

##### Risk Heat Map

Table of contents

[1 Introduction 6](#_Toc487203567)

[1.1 Context 6](#_Toc487203568)

[1.2 Document objectives 6](#_Toc487203569)

[1.3 Scope 6](#_Toc487203570)

[1.4 Audience 6](#_Toc487203571)

[1.5 Document structure 6](#_Toc487203572)

[1.6 References 6](#_Toc487203573)

[1.7 Acronyms 7](#_Toc487203574)

[1.8 Glossary 7](#_Toc487203575)

[2 Methodology and proceeding 8](#_Toc487203576)

[2.1 Methodology 8](#_Toc487203577)

[2.1.1 Context establishment 8](#_Toc487203578)

[2.1.2 Risk assessment 8](#_Toc487203579)

[Risk identification 8](#_Toc487203580)

[Risk analysis 9](#_Toc487203581)

[Risk evaluation 9](#_Toc487203582)

[2.1.3 Risk treatment 9](#_Toc487203583)

[2.1.4 Risk acceptance 9](#_Toc487203584)

[2.2 Proceeding during the analysis 10](#_Toc487203585)

[3 Context establishment 11](#_Toc487203586)

[3.1 General considerations 11](#_Toc487203587)

[3.2 Basic criteria 11](#_Toc487203588)

[3.2.1 General risk assessment criteria 11](#_Toc487203589)

[3.2.2 Impact criteria 11](#_Toc487203590)

[3.2.3 Risk acceptance criteria 11](#_Toc487203591)

[3.2.4 Description of the target 12](#_Toc487203592)

[4 Risk assessment 13](#_Toc487203593)

[4.1 Risk assessment meetings 13](#_Toc487203594)

[4.2 Risk identification 13](#_Toc487203595)

[4.2.1 Assets identification 13](#_Toc487203596)

[4.2.2 Brainstorming 13](#_Toc487203597)

[4.2.3 Threats exposure mapping 14](#_Toc487203598)

[4.2.4 Vulnerabilities exposure mapping 14](#_Toc487203599)

[4.2.5 Risk exposure mapping 14](#_Toc487203600)

[4.3 Risk analysis 14](#_Toc487203601)

[4.3.1 Risk scenarios and likelihood & impact scales 15](#_Toc487203602)

[4.3.2 Overview of the risk analysis results 15](#_Toc487203603)

[4.3.3 Typology of estimated risks 15](#_Toc487203604)

[4.4 Risk evaluation 17](#_Toc487203605)

[5 Risk treatment 18](#_Toc487203606)

[5.1 Summary of treatment plan 18](#_Toc487203607)

[5.2 Detailed risk treatment plan 19](#_Toc487203608)

[6 Risk acceptance 20](#_Toc487203609)

[7 Feedback loops of risk assessment process 20](#_Toc487203610)

[7.1 Risk communication 20](#_Toc487203611)

[7.2 Risk monitoring and review 20](#_Toc487203612)

[8 Implementation level of security measure and organisation’s compliance 21](#_Toc487203613)

[8.1 Modus operandi 21](#_Toc487203614)

[8.2 Evolution of the organisation’s compliance 22](#_Toc487203615)

[8.2.1 Compliance level for ISO/IEC 27001 22](#_Toc487203616)

[8.2.2 Compliance level for ISO/IEC 27002 23](#_Toc487203617)

[8.2.3 Compliance with specific framework 23](#_Toc487203618)

[Annex A: Details of the risk analysis 24](#_Toc487203619)

[Annex B: Implementation status of considered standards and best practices 25](#_Toc487203620)

List of figures

[Figure 1: The risk management process 8](#_Toc487203621)

[Figure 2: Risk Heat Map 15](#_Toc487203622)

[Figure 3: Number of risks by asset 15](#_Toc487203623)

[Figure 4: Number of risks by asset type 16](#_Toc487203624)

[Figure 5: Number of risks by risk scenario 16](#_Toc487203625)

[Figure 6: Number of risks by risk scenario type 17](#_Toc487203626)

[Figure 7: ISO/IEC 27001 compliance level during the different implementation phases 22](#_Toc487203627)

[Figure 8: ISO/IEC 27002 compliance level during the different implementation phases 23](#_Toc487203628)

[Figure 9: Compliance with XXXX during the different implementation phase 23](#_Toc487203629)

List of tables

[Table 1: Risk acceptance threshold 11](#_Toc487203630)

[Table 2: General considerations on the target of the risk analysis 12](#_Toc487203631)

[Table 3: List of expert meetings organised in the context of the risk assessment 13](#_Toc487203632)

[Table 4: List of assets considered in the risk analysis 13](#_Toc487203633)

[Table 5: List of assets not considered in the risk analysis 13](#_Toc487203634)

[Table 6: Risk exposure levels 14](#_Toc487203635)

[Table 7: Threat exposure estimation 14](#_Toc487203636)

[Table 8: List of vulnerabilities and its exposure level 14](#_Toc487203637)

[Table 9: Risk specificities 14](#_Toc487203638)

[Table 10: Considered risk scenarios 15](#_Toc487203639)

[Table 11: Probability scale 15](#_Toc487203640)

[Table 12: Impact scale 15](#_Toc487203641)

[Table 13: Characteristics of implementation phases 18](#_Toc487203642)

[Table 14: Risk treatment plan 19](#_Toc487203643)

[Table 15: Implementation scale of security measures. 21](#_Toc487203644)

# Introduction

## Context

The implementation of security safeguards, especially in the case of ISMS implementation, needs to perform an information risk assessment to adapt security response to current threats, business and legal security requirements in line with the organisation’s risk appetite. In that framework, Customer decided to perform a risk analysis compliant with ISO 27005 guidance using TRICK services itrust consulting web application of risk assessment.

## Document objectives

The present document presents the published results of the risk assessment performs by eomar. The last updated and applicable version of the risk assessment can be consulted using the TRICK services web application.

## Scope

The scope of this risk analysis is summary of the scope.

## Audience

The report is intended to be distributed to top management, risk owners and all involved personnel.

## Document structure

The report is structured in several chapters:

* Chapter 2 describes the used methodology of the risk assessment;
* Chapter 3 describes the context, the target and the value of assets considered;
* Chapter 4 presents the results of the risk assessment;
* Chapter 5 presents the risk treatment;
* Chapter 6 and 7 gives some mandatory information relative to the risk acceptance and feedback loop of the risk assessment management process;
* Chapter 8 describes the current and future implementation and compliance levels of the organisation regarding of relevant standards and regulations;
* Annex A presents the details of the risk analysis by indicating the considered assets, the identified risk scenarios and the results of the likelihood and impact estimations;
* Annex B includes the implementation details of security controls coming from international standards and best practices considered for the risk treatment.

## References

1. ISO/IEC 27001:2013(E) Information technology – Security techniques. Information security management system – Requirements.
2. ISO/IEC 27002:2013(E) Information technology – Security techniques – Code of practice for information security management.
3. ISO/IEC 27005:2011(E) Information technology – Security techniques – Information security risk management.

## Acronyms

|  |  |
| --- | --- |
| ISO | International Organization for Standardization |
| IEC | International Electrotechnical Commission |
| TRICK | Tool for RIsk management based on Central Knowledge base |

## Glossary

|  |  |
| --- | --- |
| MAGERIT | Risk assessment methodology published by the Spanish government. |
| Residual risk | Risk remaining after risk treatment. |
| Risk | Combination of the likelihood of an event and its consequence. |
| Risk analysis | Systematic use of information to identify sources and to estimate the risk. |
| Risk assessment | Overall process of risk analysis and risk evaluation. |
| Risk avoidance | Decision not to become involved in, or action to withdraw from, a risk situation. |
| Risk criteria | Terms of reference by which the significance of risk is assessed. |
| Risk estimation | Process used to assign values to the probability and consequences of a risk. |
| Risk evaluation | Process of comparing the estimated risk against given risk criteria to determine the significance of the risk. |
| Risk identification | Process to find, list and characterize elements of risk. |
| Risk management | Coordinated activities to direct and control an organization with regard to risk. |
| Risk reduction | Actions taken to lessen the probability negative consequences or both, associated with a risk. |
| Risk retention | Acceptance of the burden of loss, or benefit of gain from a particular risk. |
| Risk transfer | Sharing with another party the burden of loss or benefit of gain, for a risk. |
| Threat | A potential source of an incident that may result in adverse changes to an asset, a group of assets or an organization. |
| TRICK Service | Risk assessment tool developed by itrust consulting |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat. |

# Methodology and proceeding

## Methodology

The risk assessment and the definition of relative treatment plan have been conducted following the ISO/IEC 27005 risk management process as presented in Figure 1 and described below.

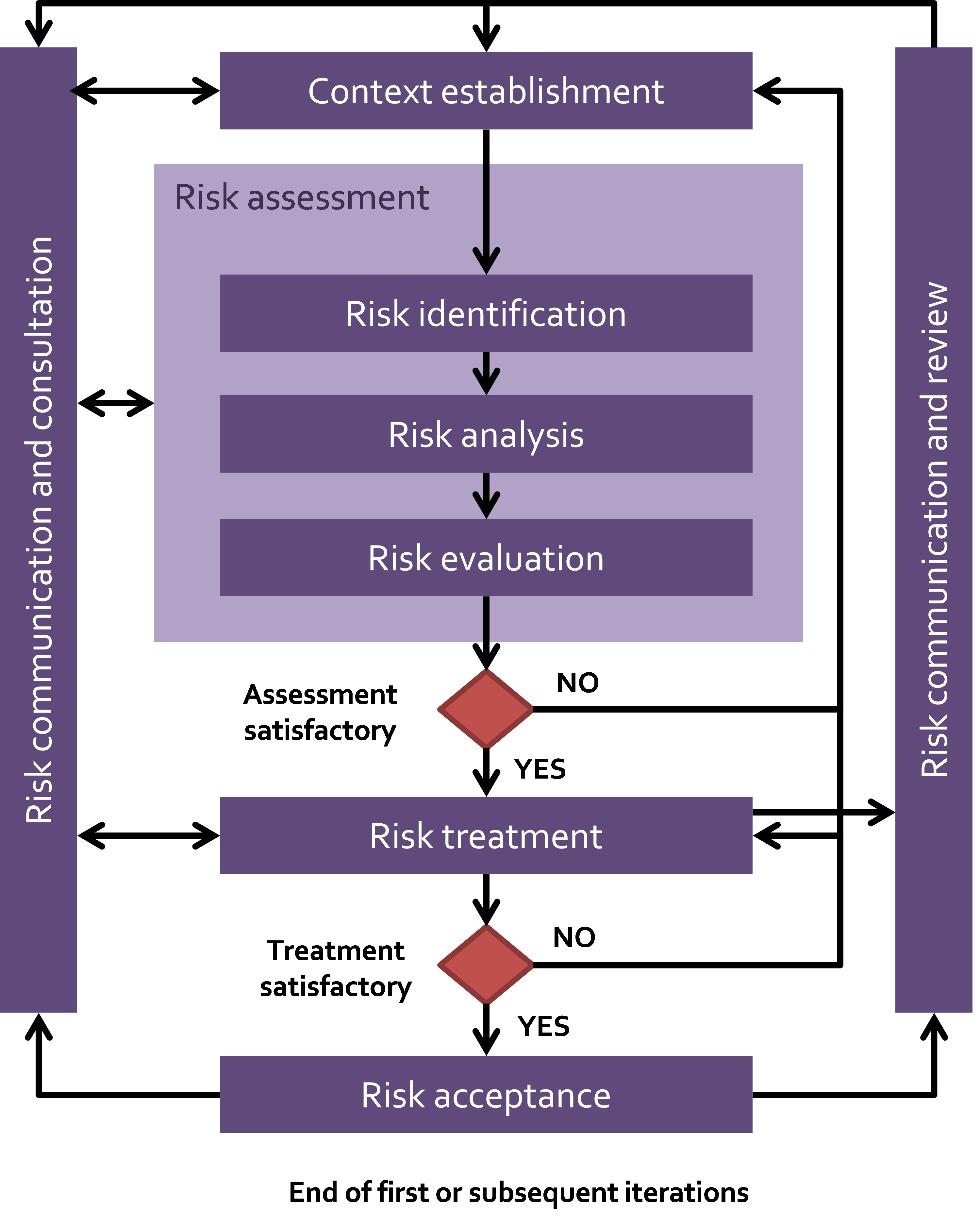


Figure 1: The risk management process

### Context establishment

This process is intended to specify the basic criteria for the risk evaluation, the target and the perimeter of this risk analysis, as well as the organisation's risk management process.

### Risk assessment

This process includes three distinct phases allowing identifying risks following their probability of occurrence and their importance.

#### Risk identification

The objective of risk identification is to determine what might cause losses, and to understand how, where and why these losses could happen. This phase prepares the risk assessment itself. It took place in the following order:

1. Identification of assets (see section 4.2.1).
2. Identification of threats (see section 4.2.3).
3. Identification of existing security measures (see Chapter 8 and **Error! Reference source not found.**).
4. Identification of vulnerabilities through identification of missing security in the previous item (See section 4.2.4).
5. Identification of consequences (impact estimated by considering the impact criteria (See Section 4.2.5).

#### Risk analysis

The risk analysis includes several phases:

1. The choice of a methodology. (see 4.3.1).
2. The assessment of the risk consequences (see 4.3.1).
3. The assessment of the risk occurrence likelihood (see 4.3.1).
4. The determination of the level of risk (see 4.3.2 and 4.3.3).

#### Risk evaluation

The process of risk evaluation uses a list of risks with indicated risk levels and risk acceptance criteria, compares them and produces a list of prioritised risks for risk treatment. Additionally, to the estimated level of risk, the process considers contractual obligation, legal aspects, and regulation issues.

### Risk treatment

The risk treatment consists in choosing measures in order to mitigate, retain, avoid, or transfer the risks, and to define a risk treatment plan.

The measure selection depends on the measures cost/benefit ratio. The risk treatment includes an indication of costs and of the risk level after the effective implementation of the risk treatment plan.

This phase produces a risk treatment plan which is a plan of the measures retained to reduce the risks and an indication of the residual risk, i.e. the risk after the implementation of the selected measures.

### Risk acceptance

This phase consists of accepting the residual risks and ensuring the responsibility that the current risk is reduced to the residual risk in an accepted way. This decision thus includes the acceptation of the risk treatment plan, which means the financial agreement and the commission of the work in order to ensure that the plan could be implemented as planned.

The decision shall be formally documented.

Note: this point is not covered by the present report and should be subject to a specific management process.

## Proceeding during the analysis

To implement pragmatically the risk assessment framework described above for Organisation name, we followed the following process:

1. Description of the risk management target;
2. Identification of the most important assets to consider;
3. Brainstorming on the exposure of the assets towards typical threats, vulnerabilities and risk specificities;
4. Identification and analysis of the current implementation level of security requirements and controls part of the following frameworks:
   1. ISO 27001
   2. ISO 27002
5. Qualitative analysis of risks linked to the considered assets;
6. Identification of security measures allowing to modify the level of risks to an acceptable level and estimation of implementation costs;
7. Validation of the risk assessment results;
8. Validation of the risk treatment plan;
9. Summary and presentation of the conclusions.

# Context establishment

This section specifies the basic criteria for the risk evaluation, the target and the perimeter of the risk analysis, as well as the risk management process.

## General considerations

The process of this risk assessment consists in performing in collaboration with the assets’ owners the high-level assessment of the risks, in refining the current risk evaluation of the information treatment systems involved in the targeted scope, in define the risk acceptance criteria, and formulate a risk treatment plan to reach the previous criteria.

The approach for the risk assessment is a combination of the following methods:

1. Identification of risks by mapping threats of MAGERIT method and documentation of countermeasures in dedicated expert meetings.
2. Qualitative estimation of risk for all critical assets with TRICK Service.
3. Evaluation of the implementation level of security measures and estimation of cost to achieve full compliance and for implementing newly identified security measures.
4. Prioritisation of security measures for the establishment of a risk treatment plan.

## Basic criteria

### General risk assessment criteria

Risks are assessed considering:

* The importance of the information essential to assure the operation of the target;
* Legal, regulatory and contractual requirements;
* The potential impacts if a risk occurs;
* All three aspects of information security, i.e. confidentiality, integrity, and availability.

### Impact criteria

The impact of a security incident is estimated considering impact categories and impact levels. When the impact is estimated, the three aspects of information security are generally considered (confidentiality, integrity and availability). However, other aspects could be considered such as loss of reputation or contractual and legal issues.

The impact categories considered in this analysis are:

### Risk acceptance criteria

The risk acceptance criteria are presented in the following table:

Table 1: Risk acceptance threshold

### Description of the target

This section describes in key terms the organisation and its main activities which are affected by this risk assessment.

Table 2: General considerations on the target of the risk analysis

# Risk assessment

The risk assessment process is composed of three distinct phases allowing to identify, analyse and evaluate the risks.

## Risk assessment meetings

The risk assessment has been performed during expert meetings. The following table enumerates the different meetings that had been organised.

|  |  |  |
| --- | --- | --- |
| Department | Participants | Date(s) of meeting(s) |
|  |  | 1. dd/mm/yy 2. dd/mm/yy 3. dd/mm/yy |
|  |  | 1. dd/mm/yy 2. dd/mm/yy 3. dd/mm/yy |
|  |  | 1. dd/mm/yy 2. dd/mm/yy 3. dd/mm/yy |

Table 3: List of expert meetings organised in the context of the risk assessment

## Risk identification

The objective of risk identification is to determine what might cause loss, and to understand how, where and why these losses could happen. This phase prepares the risk assessment itself. It took place in the following order:

1. Identification of assets;
2. Identification of threats, vulnerabilities and risk specificities (brainstorming);
3. Identification of existing security measures (see Annex B);
4. Identification of consequences that loss of confidentiality, integrity or availability may have for the considered risk assessment target (details of the risk analysis can be found in Annex A)

### Assets identification

The following table lists the assets considered as sufficiently critical to be included in the risk analysis process.

Table 4: List of assets considered in the risk analysis

The following table lists the assets not considered as sufficiently critical to be included in the risk analysis process.

Table 5: List of assets not considered in the risk analysis

### Brainstorming

During expert meetings, threats, vulnerabilities and risks logically ordered according to different criteria (MAGERIT method) are considered and assessed according to the level **++** and **+** in case organisation is very exposed, n for a normal exposition, and **-** or **--** whether the organisation is less exposed than the normal level (see Table 6 below).

The following scale has been used to express the exposition of the scope of the risk analysis:

|  |  |
| --- | --- |
| Exposition | |
| Symbol | Description |
| - - | Very weak |
| - | Weak |
| N | Normal |
| + | Important |
| + + | Very important |

Table 6: Risk exposure levels

### Threats exposure mapping

A vulnerability can only become a risk if there exist threats that exploit the vulnerability. For this, it is very important to know the threats for which the target to analyse is exposed. The following table provides an overview of the exposure levels towards typical threats.

Table 7: Threat exposure estimation

### Vulnerabilities exposure mapping

A threat can only become a risk if there are vulnerabilities that can be exploited by the threat. For this, it is very important to know the vulnerabilities of the target to analyse to be able to plan corrective and preventive measures to avoid such an exploitation of a vulnerability by a threat.

Table 8: List of vulnerabilities and its exposure level

### Risk exposure mapping

After considering general aspects in the mapping of threats and vulnerabilities, we have considered the threats grouped by source, to roughly estimate the exposure of the company against these threats. This evaluation considers not only the strength and frequency of the threat, but also the level of vulnerability of targeted assets and the impact on the company.

Table 9: Risk exposure estimation

## Risk analysis

The risk analysis includes several phases:

1. The choice of a methodology.
2. The assessment of the risk consequences following a defined scale.
3. The assessment of the risk occurrence likelihood following a defined scale.
4. The determination of the level of risk (see Annex A for details).

### Risk scenarios and likelihood & impact scales

In this stage, the risks have been qualified with the help of TRICK Service. The assessment was based on generic risk scenarios described below and regrouping the most essential threats and vulnerabilities in relation to the three information security aspects: Confidentiality, Integrity and Availability have been quantified.

Table 10: Considered risk scenarios

For each scenario, the consultant in collaboration with business line responsible will assess the qualitative perception of impact and of likelihood of the scenarios for the organisation to estimate the identified risk. The following tables present the likelihood and impact scales used.

Table 11: Probability scale

Table 12: Impact scale

### Overview of the risk analysis results

The risk analysis results are illustrated in the following risk heat map. This map depicts for each risk sector defined by a certain qualitative level of impact and likelihood, how many assets are part of. The detail for each asset of the risk analysis in terms of impact level, likelihood level and description of the assessment is enclosed in the Annex A: *Details of the risk analysis*.

Figure 2: Risk Heat Map

### Typology of estimated risks

This section includes figures that illustrate which assets and asset types are most exposed to risks (Figure 3 and Figure 4) and from which risk scenarios and risk scenario types most risks are resulting from (Figure 5 and Figure 6).

Figure 3: Number of risks by asset

Figure 4: Number of risks by asset type

Figure 5: Number of risks by risk scenario

Figure 6: Number of risks by risk scenario type

## Risk evaluation

The risk evaluation allows to compare the results of the risk analysis with the risk acceptance criteria that have been defined together with the stakeholders (see section 3.2.3).

Risk evaluated to be non-acceptable must be treated by defining a risk treatment plan.

# Risk treatment

To treat the identified non-acceptable risks, a list of security measures to be implemented have been drawn. The list is based on international standards and best practices and is ordered to define a risk treatment plan. The implementation of this risk treatment plan allows to reduce the risks to an acceptable level.

The risk treatment includes an indication of the risk level after the effective implementation of the risk treatment plan. The treatment plan is defined in several phases to improve step by step the security to reach an chosen risk level in acceptable time duration and considering the organisation resources.

## Summary of treatment plan

The table below gives the summary of the main characteristic of the treatment plan for each phase. The table described for each phase the following information:

* **The phase characteristic**:
  + The start and end date of the phase;
  + The implementation rate of the security measure according to chosen standard and regulation frameworks;
  + The number of security measures whose implementation reached 100% at the end of the phase;
* **The average annual cost of the phase** (considering set-up cost, lifetime and yearly maintenance;
* **The resources planning i.e.:**
  + The implementation costs of the security measures (set-up cost) including:
    - Internal workload in man-days;
    - External workload in man-days;
    - Investment in kilo-euros
    - The total of implementation cost in kilo-euros.
  + The recurrent costs to be planned to maintain the security measures:
    - Internal maintenance workload in man-days;
    - External maintenance workload in man-days;
    - Recurrent investments to maintain implementation rate in kilo-euro;
    - The total of recurrent costs in kilo-euros;
  + The total cost of the phase including internal and external workload.

Note: ⯍ l one external man-day costs **0** € and an internal man-day costs **0** €.

⯍ l that the average cost is different from the set-up cost plus recurrent costs as they consider a lifetime for each investment.

Table 13: Characteristics of implementation phases

## Detailed risk treatment plan

In the following, we provide a list of security measures planned to be implemented to treat the identified non-acceptable risks. This list enhanced with deadlines and responsibilities and is called the risk treatment plan according to ISO/IEC 27001. The list contains a sequence number, the reference towards the standard/best practice the security measures come from, a description of what remains to be done, the residual risk after implementation of the measure (including all previous measures), the annual cost in days of internal work and the cost in days of external consultants to implement the measure and the investment budget for extra measure. The last column assigns the phase in which the measure is planned to be implemented.

Table 14: Risk treatment plan

# Risk acceptance

This phase consists of accepting the residual risks and ensuring the responsibility that the current risk is reduced to the residual risk in an accepted way. This decision thus includes the acceptation of the risk treatment plan, which means the agreement on needed resources and the commission of the work to ensure that the plan can be implemented as planned.

The decision shall be formally documented.

# Feedback loops of risk assessment process

## Risk communication

The underlying report or parts of it are used to exchange risk related information. The risk communication strategy is not part of the present report.

## Risk monitoring and review

This process is not part of the underlying report. Risk monitoring and review consists of updating this report annually or in case of significant changes and identification of important risks.

# Implementation level of security measure and organisation’s compliance

This chapter gives additional information regarding the risk assessment process. It describes the modus operandi to establish the security measures to be applied to the organisation in terms of information security:

1. to identify the security measures to implement to ensure the information security of the organisation according to applicable standards, regulations and security good practices
2. to assess the current implementation level of security measures.
3. to assess the needed resources (calculated in kilo-euros) to fully implement these measures in the organisation.

This information has been used in treatment plan establishment process and allows describing the evolution of organisation compliance level from now to the end of the treatment plan implementation.

## Modus operandi

To identify the security measures, to assess both their current level of implementation and the resource needed to fully implement them, the consultant described within TRICK service tool, for the exhaustive list of security measures included in the chosen standards, regulations and good security practices, the following information:

* **Ref**: the reference of security control;
* **Domain:** the area (and title);
* **ST**: the status i.e. **AP** if applicable, **NA** if not applicable, or **OB** if mandatory;
* **IR**: the rate of implementation (indicating what percentage of the measure is already operational); the following rules of assessment is applied to provide the reliability of the assessment.:

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Description | Criteria |
| Implementation rate | **0%** | The measure is neither implemented nor identified in the SI security framework for the considered domain. | Lack of consideration and implementation of the measure. |
| **20%** | The measure has been identified in the SI security framework but is informally implemented. | Measure included in the security plan. Technical measures but unstructured (mainly based on current professional expertise). |
| **50%** | The implementation of the measure has been decided and a formal implementation is largely started. | Implementation plan for the measure. Main aspect already implemented according to the plan. |
| **80%** | The measure is implemented according to a formal plan but not entirely or long-term management shall be checked and consolidated. | Implementation compliance with formal security plan and almost finished. Finalisation and control has to be done. |
| **100%** | The measure is entirely implemented and well managed according to the security plan set up for the considered security domain. | Implementation of the measure compliance with security plan, checked and under control. |

Table 15: Implementation scale of security measures.

* **IW**: the internal set-up workload, showing how many days of internally work are necessary to implement the security measure at 100%;
* **EW**: the external set-up showing how many days of work of a service provider is needed to implement the security measure at 100%;
* **INV**: the investment budget in k€ indicating what is expected in addition to internal and external resources to implement the measure at 100%;
* **LT**: the lifetime in years of the measure;
* **IM**: the yearly internal workload to maintain the security measure;
* **EM**: the yearly external workload to maintain the security measure;
* **RI**: the recurrent investments for maintaining the security measure;
* **CS**: the annual cost in k€, calculated from the previous settings (taking into account the average cost of one internal man-day and of one external man-day;
* **Comment**: a justification of the provided estimates;
* **To do**: a description of the actions to be done to achieve full compliance.

The complete assessment can be found in *Annex B: Implementation status of considered standards and best practices*.

## Evolution of the organisation’s compliance

### Compliance level for ISO/IEC 27001

During the risk assessment process of the organisation, the requirement of ISO/IEC 27001 has been assessed in the order of appearance in the standard. The numbers refer to the chapter number. The following graph gives an overview on the average compliance rate for each chapter.

Figure 7: ISO/IEC 27001 compliance level during the different implementation phases

### Compliance level for ISO/IEC 27002

During the risk assessment process of the organisation, all 114 of ISO/IEC 27002 have also been considered. The following figure represents the compliance level of the different ISO/IEC 27002 chapters during the different implementation phases.

Figure 8: ISO/IEC 27002 compliance level during the different implementation phases

# Annex A: Details of the risk analysis

The following table includes the risk estimation for each pair of asset and threat:

* The impact when the threat occurs on the asset;
* The probability of the occurrence of the threat within one year.

The risk importance level is computed by multiplying the maximal impact with the probability of occurrence for all risk scenarios.

# Annex B: Implementation status of considered standards and best practices

The following tables include for each security measure its current implementation rate and the workload to invest to fully implement the security measures. The implementation rate and the costs for the security measures which are not fully implemented were estimated.

For each security measure, we indicate:

* **Ref**: the reference of security control;
* **Domains**: the area (and title);
* **ST**, the status (AP = applicable, NA not applicable, M: mandatory);
* **IR**: the rate of implementation (indicating what percentage of the measure is already operational);
* **IW**: the internal set-up workload, showing how many days of internally work are necessary to implement the security measure;
* **EW**: the external set-up showing how many days of work of a service provider is needed to implement the security measure;
* **INV**: the investment budget in k€ indicating what is expected in addition to internal and external resources to implement the measure;
* **LT**: the lifetime in years of the measure;
* **IM**: the yearly internal workload to maintain the security control;
* **EM**: the yearly external workload to maintain the security control;
* **RINV**: the recurrent investments for maintaining the security control;
* **CS**: the annual cost in k€, calculated from the previous settings (taking into account the average cost of one internal man-day and of one external man-day);
* **Comment**: a justification of the provided estimates;
* **To do**: a description of the actions to be done to achieve full compliance;
* **Resp**: The person(s) responsible for the implementation of the security measure.