|  |  |
| --- | --- |
|  |  |
| Organisation name | |
| Title of the project | |
| **Risk analysis report** | |
|  | |

General information

|  |  |
| --- | --- |
| Sequence number | Q139 |
| Version | 4.8.7 |
| State | Draft |
| Approved by | …. |
| Date of approval | 06/03/18 |
| Classification | Internal |

Distribution list

|  |  |  |  |
| --- | --- | --- | --- |
| Recipient | Date | Channel | Reason |
| … | … | Choose | Choose |
| … | … | Choose | Choose |

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Modifications |
| 0.1 | … |  |  |
| 0.2 | … |  |  |

Working group

|  |  |
| --- | --- |
| Name | Organisation |
| Customer working group | Customer |
| itrust working group | itrust consulting |

Approbations

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

Management summary

##### Context

The following document presents the results of the 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 summarize the scope here

##### 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.

##### Considered assets and relative risk evaluation

The considered assets have a total value of 0 k€ and the total sum of the risks the organisation is currently exposed to the relative scope is estimated to **0** k€ per year (ALE).

|  |  |  |
| --- | --- | --- |
| Type of asset | Value by type of asset (k€) | Risk by type of asset (k€/year) |
| Information |  | 0 |
| Software | 0 | 0 |
| Hardware | 0 | 0 |
| Network | 0 | 0 |
| Human Resource | 0 | 0 |
| Service | 0 | 0 |
| Business process | 0 | 0 |
| Compliance | 0 | 0 |
| Financial | 0 | 0 |
| Immaterial | 0 | 0 |
| Total | 0 k€ | 0 k€/year |

##### Current security level

The implementation level of security is 0 % according to the requirements of the relevant standard and regulations. We shall note that this implementation level of the security measures described in the relevant standard and regulations shall be upper than 0 % to ensure a security level compliant with the minimum-security requirements regarding the relevant standards and regulations.

##### Risk treatment plan

The risk treatment plan is composed of 0 implementation phases:

The average annual Return On Security Investment (ROSI) due to security measures implementation is 0 k€ for the overall treatment plan. This treatment plan will allow to reach a relative ROSI of  0 % which means that for 1 € spent for security improvement, the expected loss due to incidents happened without this investment, will decrease of 0.1 €.

The annual loss expectancy should pass from **0** k€ to 0 k€ at the end of the overall treatment phases, which is less than the acceptable risk level expected by the organisation.

Table of contents

[1 Introduction 6](#_Toc487100884)

[1.1 Context 6](#_Toc487100885)

[1.2 Document objectives 6](#_Toc487100886)

[1.3 Scope 6](#_Toc487100887)

[1.4 Audience 6](#_Toc487100888)

[1.5 Document structure 6](#_Toc487100889)

[1.6 References 6](#_Toc487100890)

[1.7 Acronyms 7](#_Toc487100891)

[1.8 Glossary 7](#_Toc487100892)

[2 Methodology and proceeding 8](#_Toc487100893)

[2.1 Methodology 8](#_Toc487100894)

[2.1.1 Context establishment 8](#_Toc487100895)

[2.1.2 Risk assessment 8](#_Toc487100896)

[Risk identification 8](#_Toc487100897)

[Risk analysis 9](#_Toc487100898)

[Risk evaluation 9](#_Toc487100899)

[2.1.3 Risk treatment 9](#_Toc487100900)

[2.1.4 Risk acceptance 9](#_Toc487100901)

[2.2 Proceeding during the analysis 10](#_Toc487100902)

[3 Context establishment 11](#_Toc487100903)

[3.1 General considerations 11](#_Toc487100904)

[3.2 Basic criteria 11](#_Toc487100905)

[3.2.1 General risk assessment criteria 11](#_Toc487100906)

[3.2.2 Impact criteria 11](#_Toc487100907)

[3.2.3 Risk acceptance criteria 11](#_Toc487100908)

[3.3 Description of the target 12](#_Toc487100909)

[4 Risk assessment 13](#_Toc487100910)

[4.1 Risk assessment meetings 13](#_Toc487100911)

[4.2 Risk identification 13](#_Toc487100912)

[4.2.1 Asset identification 13](#_Toc487100913)

[4.2.2 Brainstorming 14](#_Toc487100914)

[4.2.3 Threats exposure mapping 14](#_Toc487100915)

[4.2.4 Vulnerabilities exposure mapping 14](#_Toc487100916)

[4.2.5 Risk exposure mapping 14](#_Toc487100917)

[4.3 Risk analysis 14](#_Toc487100918)

[4.3.1 Risk scenarios and likelihood & impact scales 15](#_Toc487100919)

[4.3.2 Overview of the risk analysis results 15](#_Toc487100920)

[4.3.3 Typology of estimated risks 15](#_Toc487100921)

[4.4 Risk evaluation 17](#_Toc487100922)

[5 Risk treatment 18](#_Toc487100923)

[5.1 General consideration regarding the identification of measures. 18](#_Toc487100924)

[5.1.1 Parameter tuning and outcome’s validation 18](#_Toc487100925)

[5.1.2 A methodology based on profitability 18](#_Toc487100926)

[5.2 Summary of treatment plan 18](#_Toc487100927)

[5.3 Increase of compliance rate and rentability of the phases 19](#_Toc487100928)

[5.4 Detailed risk treatment plan 20](#_Toc487100929)

[6 Risk acceptance 21](#_Toc487100930)

[7 Feedback loops of risk assessment process 21](#_Toc487100931)

[7.1 Risk communication 21](#_Toc487100932)

[7.2 Risk monitoring and review 21](#_Toc487100933)

[8 Implementation level of security measures and organisation’s compliance 22](#_Toc487100934)

[8.1 Modus operandi 22](#_Toc487100935)

[8.2 Evolution of the organisation’s compliance 23](#_Toc487100936)

[8.2.1 Compliance level for ISO/IEC 27001 23](#_Toc487100937)

[8.2.2 Compliance level for ISO/IEC 27002 24](#_Toc487100938)

[Annex: List of security measures applicable to the TOE 25](#_Toc487100939)

List of figures

[Figure 1: The risk management process. 8](#_Toc487100940)

[Figure 2: Annual Loss Expectancy by assets. 16](#_Toc487100941)

[Figure 3: Annual Loss Expectancy by asset types. 16](#_Toc487100942)

[Figure 4: Annual Loss Expectancy by Risk scenario. 17](#_Toc487100943)

[Figure 5: Annual Loss Expectancy by threat type. 17](#_Toc487100944)

[Figure 6 : Rentability of the treatment plan 19](#_Toc487100945)

[Figure 7: ISO/IEC 27001 compliance levels during the different implementation phases. 23](#_Toc487100946)

[Figure 8: ISO/IEC 27002 compliance levels during the different implementation phases. 24](#_Toc487100947)

List of tables

[Table 1: General considerations on the target of the risk analysis. 12](#_Toc487100948)

[Table 2: List of expert meetings organised in the context of the risk assessment 13](#_Toc487100949)

[Table 3: List of assets considered in the risk analysis. 13](#_Toc487100950)

[Table 4: List of assets not considered in the risk analysis. 13](#_Toc487100951)

[Table 5: Risk exposure levels 14](#_Toc487100952)

[Table 6: Threat exposure estimation. 14](#_Toc487100953)

[Table 7: List of vulnerabilities and its exposure level. 14](#_Toc487100954)

[Table 8: Risk specificities. 14](#_Toc487100955)

[Table 9: Considered risk scenarios. 15](#_Toc487100956)

[Table 10: Probability scale. 15](#_Toc487100957)

[Table 11: Impact scale. 15](#_Toc487100958)

[Table 12: Characteristics of implementation phases. 19](#_Toc487100959)

[Table 13: Risk treatment plan. 20](#_Toc487100960)

[Table 14: Implementation scale of security measures. 22](#_Toc487100961)

# 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 summarize the scope here.

## Audience

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

## Document structure

Structure of the following 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;
* The Annex includes the implementation details of security measures 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

|  |  |
| --- | --- |
| ALE | Annual Loss Expectancy. |
| MAGERIT | Risk Analysis and Management Methodology for Information Systems (risk analysis methodology of the Spanish government). |
| ROSI | Return On Security Investment. |
| TRICK | Tool for Risk management based on Central Knowledge base |

## Glossary

|  |  |
| --- | --- |
| Annual Loss Expectancy | Metric to compare risks (in €). |
| Information Security Management System (ISMS) | That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. |
| Process | Set of interrelated or interacting activities which transform inputs into outputs. |
| 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 characterise elements of risk. |
| Risk management | Coordinated activities to direct and control an organisation with regard to risk. |
| Risk optimisation | Process related to a risk to minimise the negative and to maximise the positive consequences and their respective probabilities. |
| 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. |
| ROSI | Return on investment of a security project obtained as the difference between the change in risk before and after the introduction of security measure (Delta ALE) and the annual cost of this measure. |
| Threat | A potential source of an incident that may result in adverse changes to an asset, a group of assets or an organisation. |
| 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 the 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).
2. Identification of threats (see section 4.2.3).
3. Identification of existing security measures (see Chapter 5 and Annex).
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.
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. Definition of the risk assessment target.
2. Identification of the most important assets to consider.
3. Classification and estimation of the value of the selected assets.
4. Analysis of the current implementation level of security requirements and controls part of the following frameworks:
   1. ISO 27001
   2. ISO 27002
5. Identification and estimation on the added value of security controls to be implemented with the help of TRICK Service.
6. Validation of the results.
7. Validation of the risk treatment plan.
8. 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 analysis 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 during dedicated expert meetings.
2. Quantitative estimation of risk for all critical assets with TRICK Service.
3. Evaluation of the implementation level of security controls and estimation of cost to achieve full compliance.
4. Estimation of the profitability of the security measures with TRICK Service.
5. Group of missing security measures in different implementation phases and 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;
* Direct financial consequences;
* All three aspects of information security i.e. confidentiality, integrity, and availability.

### Impact criteria

Impact of a security incident is estimated in terms of costs. When this estimation is too uncertain, impact is estimated considering a category: vital, extremely serious, very serious, serious, minor, insignificant. Although apparently qualitative, this scale will be defined as a logarithmic scale with a fixed cost for each level, corresponding to the representation of the potential lost in case of such impact. These levels will be generally linked to a percentage of the business turnover and the condition to maintain the activities of the organisation.

Note: even if this impact evaluation will be generally based on the impact of security properties loss such as confidentiality, integrity and availability of asset, the estimated impact costs will also include costs due to the loss of reputation or contractual and legal issues.

### Risk acceptance criteria

The risk acceptance criteria are defined as followed:

1. The risks for which the organisation exposition is considered weak or very weak according to the first risk assessment step (MAGERIT method cf. Table 5) are accepted and not explicitly considered in the treatment risk.
2. The risks for which the organisation exposition is considered as important or very important according to the first risk assessment step require an identification of feasible countermeasures. The risks are accepted if the responsible of Organisation name has formally been informed, and after they have formally granted the implementation of the identified countermeasures.
3. The risks considered as normal according to the first risk assessment step are accepted if responsible of Organisation name is aware of the quantitative risk estimation of typical risk scenarios covering these risks and if:
   1. Either all security measures anticipated by considered standards and assessed as profitable are planned;
   2. Or there are enough measures planned so that the estimated annual loss expectancy is lower than \*\*.\* k€.

Note: a temporary level of risks of \*\*.\* k€ upper than the previous limit can also be accepted if an risk treatment plan lowering the risk below the previous identified risk level within \*\* months, has been formally approved by the organisation.

## Description of the target

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

Table 1: 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 2: 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);
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)

### Asset identification

The following table lists the assets considered as sufficiently critical to be included in the risk analysis process. For each asset, a value has been estimated. The value represents the purchase price and / or the efforts to invest to (re-)create the asset.

Table 3: 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 4: 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.

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

Table 5: Risk exposure levels

### Threats exposure mapping

During this step, different threats have been taken into account. In order to ensure that the list of considered threats is sufficiently complete, the threats have been classified following the MAGERIT method. For each threat, the exposure of Organisation name towards this threat, compared to other companies has been estimated. The exposure level is estimated qualitatively with the help of the scale presented in Table 1.

Table 6: 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 in order to be able to plan corrective and preventive measures to avoid such an exploitation of a vulnerability by a threat.

Table 7: 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 sources, 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 8: 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 quantified with the help of TRICK Service. The annual losses for the 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 9: Considered risk scenarios.

The estimation of the risks should be performed by the consultant in collaboration with business line responsible, by considering the potential financial loss if the risk occurs. However, during this process, a quantitative estimation is sometimes too uncertain. Then, we rely on a qualitative estimation of probability or impact. To establish a financial statement of expected losses and the cost-effectiveness measures, we translate the qualitative estimation into a quantitative estimation with the scales below.

Table 10: Probability scale.

Table 11: Impact scale.

### Overview of the risk analysis results

The following table shows for each pair of assets and threat:

* The impact when the threat occurs on the asset (in kilo euros or using the value of the impact scale);
* The probability of the occurrence of the threat within one year.

These estimations allowed to compute the Annual Loss Expectancy (ALE) which represents the current financial risk of the organisation regarding the information security. The ALE the is computed by multiplying the impact with the probability of occurrence per year, and the ALE for each asset is obtained by adding the ALE for all risk scenarios.

### Typology of estimated risks

This section includes figures that illustrate which assets and asset types are most exposed to risks (Figure 2 et Figure 3) and from which risk scenarios and risk scenario types most risks are resulting from (Figure 4 et Figure 5).

Figure 2: Annual Loss Expectancy by assets.

Figure 3: Annual Loss Expectancy by asset types.

Figure 4: Annual Loss Expectancy by Risk scenario.

Figure 5: Annual Loss Expectancy by threat 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 chosen and ordered to define a risk treatment plan using the TRICK service tool. 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.

## General consideration regarding the identification of measures.

### Parameter tuning and outcome’s validation

Trick Service Tool contains multiple parameters estimating the effect of all on different risk scenarios. Those parameters have been discussed and agreed by several experts and have been the basis for the risk reduction estimate of several previous customers of itrust.

The outcome was considered to be plausible during the validation phase.

### A methodology based on profitability

Using the TRICK Service methodology of itrust consulting, we estimated the risk reductions for the various measures that are to be implemented. We derived a first-risk treatment plan in which all missing controls are implemented in the same period. We then decided to consider several implementation phases. Then, based on resource availability, interdependencies, and preference for quick wins, and ROSI, we put each security action in one of the implementation phase. This was done in several iterative steps until the risk treatment plan was plausible and achievable. In the following, we present this proposed risk treatment plan in a top-down approach.

## 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 compliance level with the applied standard;
  + The number of to be implemented during the phase;
  + The number of whose implementation reached 100% with regard to the applied standard at the end of the phase.
* **The profitability of the planned security measures:**
  + The Annual Loss Expectancy in k€ at the end of the phase (P0 giving the current ALE);
  + The Risk Reduction in kilo euros (i.e. ALE before – ALE after the implementation);
  + The average annual cost of the phase (considering set-up cost, lifetime and yearly maintenance);
  + The Return on security investment (ROSI) in k€ i.e. ROSI = Risk reduction (∆ALE) - average annual cost.
  + The relative ROSI in %, which is the ROSI divided by the total cost of implementation.
* **The resources planning**:
  + 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.

The range and the efficiency of each phase are described in the following table:

Table 12: Characteristics of implementation phases.

## Increase of compliance rate and rentability of the phases

The following figure shows the evolution of both rentability for applied measures and compliance rate according to the implementation of security measures during the defined phases.

Figure 6 : Rentability of the treatment plan

## Detailed risk treatment plan

In the following, we provide a list of missing security measures according to chosen standard and regulations guidelines. This list enhanced with deadlines and responsibilities is called the risk treatment plan according to ISO 27001. It contains a sequence number, the reference towards the standard the security measure comes from, a description of what remains to be done, the residual risk after the implementation of the measure (including all previous measures), the profitability of the measure, 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 13: 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 measures 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 14: 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: *List of security measures applicable to the TOE*.

## 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 levels 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 levels during the different implementation phases.

# Annex: List of security measures applicable to the TOE

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 of the security measures which are not yet 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.