**C:\Users\juan\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Logo_caseslu.emf**

**${DOCUMENT}**

**${COMPANY}**

**Information security -**

**MONARC**

**General information**

Version : ${VERSION}

Document status: ${STATE}

Classification : ${CLASSIFICATION}

Company: ${COMPANY}

Document name: ${DOCUMENT}

Date : ${DATE}

Security consultant(s): ${SMILE}

Client representative(s): ${CLIENT}

**Summary**

${SUMMARY\_EVAL\_RISK}

**Current risks map**

${CURRENT\_RISK\_MAP}

**Target risks map**

${TARGET\_RISK\_MAP}

Contents

[1 Introduction 4](#_Toc102393704)

[1.1 Placing the risk analysis in context 4](#_Toc102393705)

[1.2 Aims of the document 4](#_Toc102393706)

[1.3 References 4](#_Toc102393707)

[1.4 Acronyms/Glossary 4](#_Toc102393708)

[1.5 Description of the “CASES Optimised Risk Analysis Method” (MONARC) 5](#_Toc102393709)

[2 Context Establishment 7](#_Toc102393710)

[2.1 Description of the context 7](#_Toc102393711)

[2.2 Definition of the risk evaluation criteria 7](#_Toc102393712)

[2.2.1 Information risks 7](#_Toc102393713)

[2.2.1.1 Impact scale 7](#_Toc102393714)

[2.2.1.2 Threat scale 7](#_Toc102393715)

[2.2.1.3 Vulnerability scale 7](#_Toc102393716)

[2.2.1.4 Risk acceptance thresholds 8](#_Toc102393717)

[2.2.2 Operational risks 8](#_Toc102393718)

[2.2.2.1 Impact scale 8](#_Toc102393719)

[2.2.2.2 Likelihood scale 8](#_Toc102393720)

[2.2.2.3 Risk acceptance thresholds 8](#_Toc102393721)

[2.3 Evaluation of trends and threats 9](#_Toc102393722)

[3 Context Modelling 10](#_Toc102393723)

[3.1 Identifying the assets 10](#_Toc102393724)

[3.2 Identifying the vulnerabilities 10](#_Toc102393725)

[3.3 Assessing the consequences 10](#_Toc102393726)

[4 Evaluation and treatment of risks 11](#_Toc102393727)

[4.1 Summary of the risk evaluation 11](#_Toc102393728)

[4.1.1 Information risks 11](#_Toc102393729)

[4.1.2 Operational risks 11](#_Toc102393730)

[4.2 Risk treatment 12](#_Toc102393731)

[4.2.1 Kind of treatment 12](#_Toc102393732)

[4.2.2 Treatment plan 12](#_Toc102393733)

[Appendix A: Interview and information collection 13](#_Toc102393734)

[Appendix B: Evaluation of trends 14](#_Toc102393735)

[Appendix C: Evaluation of threats 15](#_Toc102393736)

[Appendix D: Asset context 16](#_Toc102393737)

[Appendix E: Risk owners 17](#_Toc102393738)

[Appendix F: Notes and comments from the consultant 18](#_Toc102393739)

[Information risks 18](#_Toc102393740)

[Operational risks 19](#_Toc102393741)

# Introduction

## Placing the risk analysis in context

${CONTEXT\_ANA\_RISK}

## Aims of the document

This document provides a summary of the method and presents the results of the risk analysis carried out with MONARC in the client's environment. MONARC follows the international ISO 27005:2011 standard.

The results obtained aim to identify the major risks, understand the level of security in place and provide recommendations for implementing security measures. The parties recognise that the recommendations are neither exclusive nor exhaustive.

The list of risks found is based on the information provided by the Client and/or its representatives, with no further verifications carried out. SMILE GIE may not be held liable for any omissions or errors that result from analysis of this assessment which may be due any involved or a third party.

## References

1. ISO/IEC 27005 (2011), Management of the risks associated with information security.
2. <http://www.iso.org/iso/en/catalogue_detail?csnumber=56742>. The ISO 27005 standard explains in detail how to carry out a risk assessment and address risks in relation to information security

## Acronyms/Glossary

**Asset:** Any item of value to the institution.

**Confidentiality**: The attribute that information is not available or disclosed to unauthorised individuals, entities or processes.

**Availability**: The attribute of being accessible and usable upon request from an authorised entity.

**Integrity**: The attribute of preserving the accuracy and completeness of an item.

**MONARC**: CASES Optimised Risk Analysis Method.

## Description of the “CASES Optimised Risk Analysis Method” (MONARC)

The MONARC risk analysis method is composed of four phases:



More specifically:



MONARC simplifies risk management by offering a risk management solution as well as information security governance, based on industry standards. It allows for analysis from existing and customisable models to be made in a short amount of time, while remaining compliant with the ISO/IEC 27005:2011 international standard.

MONARC is based on a library of risk models offering objects made of risk scenarios by assets or groups of assets. This approach facilitates the management of the most common risks and allows for benefits in objectivity as well as efficiency. As MONARC is completely repeatable, these results can be intensified and adjusted to the maturity of each organisation by increasing the depth of risk scenarios.

**Context Establishment**

The first step is to take stock of the context, challenges and priorities of the company or organization that wishes to analyse its risks. This particularly serves to identify key activities and critical processes of the business in order to guide the risk analysis towards the most important elements. To do this, a kick-off meeting is organized with the members of the management and key individuals. The goal is to know what makes the company «live» and what could destroy it, to identify the key processes, the internal and external threats as well as organisational, technical and human vulnerabilities.

**Context Modelling**

This phase includes the modelling of objects and trees. The assets were identified in the previous phase. They must now be detailed and formalised in a diagram that displays their interdependencies.

Impacts are defined at the level of the primary assets (processes or information), following the information gathered in the context establishment phase. The secondary assets inherit the impact of the primary asset to which they are attached (object tree). The impact level of the secondary assets can be modified manually.

**Evaluation and treatment of risks**

The assessment consists of quantifying the threats, vulnerabilities and impacts in order to calculate the risks.

To do this, it is necessary to have quality information about the exact likelihood of the threats, the ease of exploitation of vulnerabilities and potential impacts; hence the need to rely on metrics that have been validated by experts.

When the risk assessment identifies a risk that is higher than the acceptable level (risk acceptance grid), risk treatment measures should be implemented in order to reduce the risk down to an acceptable level.

**Implementation and monitoring**

When the first treatment of risks has been carried out, an ongoing management phase with security monitoring and recurring control of security measures must be entered, in order to improve it in a sustainable manner.

This fourth phase also allows to continuously optimise security by increasing the detail of objects used and by expanding the scope of the risk analysis.

# Context Establishment

## Description of the context

${CONTEXT\_GEST\_RISK}

## Definition of the risk evaluation criteria

### Information risks

### Impact scale

The table below shows the scale of impacts and consequences that may pose a risk for the institution. 0 represents no impact, so there is no risk.

${SCALE\_IMPACT}

### Threat scale

The table below shows the scale of probability that a threat will occur.

${SCALE\_THREAT}

### Vulnerability scale

The table below shows the scale of vulnerability for the asset in question. The assessment of vulnerability takes into account the security measures in place.

${SCALE\_VULN}

### Risk acceptance thresholds

The table below shows risk calculations. The colours are for information purposes and should be accepted and/or modified by the Board of Directors / Executive Committee.

Red: An unacceptable risk that requires action

Orange: An average risk which may or may not require action, depending on the case

Green: Low risk that requires no action

${TABLE\_RISKS}

### Operational risks

### Impact scale

${OP\_RISKS\_SCALE\_IMPACT}

### Likelihood scale

${OP\_RISKS\_SCALE\_LIKELIHOOD}

### Risk acceptance thresholds

${TABLE\_OP\_RISKS}

## Evaluation of trends and threats

${SYNTH\_EVAL\_THREAT}

The table below shows threats that have required particular attention.

${TABLE\_THREATS}

# Context Modelling

## Identifying the assets

${SYNTH\_ACTIF}

## Identifying the vulnerabilities

Using MONARC modelling and its objects enables vulnerabilities to be identified in sufficient detail for repeated risk analysis.

It is, however, up to the discretion of the consultants to include new contextual risks that they discover during the assignment.

## Assessing the consequences

The table below shows the impacts for the essential assets of ${COMPANY}.

To save time, all the secondary assets that will be entered into the essential asset model will receive these impacts by default, which can then be adjusted manually.

${IMPACTS\_APPRECIATION}

# Evaluation and treatment of risks

The results of the collection of diverse information, encoding and evaluations are processed in the MONARC software and are available to the client. Some of this information can also be found appended to this document.

The next part of this chapter presents the results and recommendations that complete this risk analysis.

## Summary of the risk evaluation

${SUMMARY\_EVAL\_RISK}

### Information risks

${DISTRIB\_EVAL\_RISK}

${GRAPH\_EVAL\_RISK}

### Operational risks

${DISTRIB\_EVAL\_OP\_RISK}

${GRAPH\_EVAL\_OP\_RISK}

## 

## Risk treatment

### Kind of treatment

${RISKS\_KIND\_OF\_TREATMENT}

### Treatment plan

The following table contains the main recommendations that arise from the risk analysis and the risk treatment plan. The evaluation and development of recommendations use the following scale:

●●● : Recommendation that requires rapid action.

●● : Recommendation that requires dedicated action to remedy a vulnerability or a good practice that is shown to be lacking.

● : Useful information for security, advice.

Information risks

${RISKS\_RECO\_FULL}

Operational risks

${OPRISKS\_RECO\_FULL}

# Appendix A: Interview and information collection

The information that made this analysis possible was collected through interviews with key staff for the area in question technical managers.

We would like to thank the following people for their active contributions during the interviews and the visits conducted in connection with our assignment listed below:

${TABLE\_INTERVIEW}

# Appendix B: Evaluation of trends

${TABLE\_EVAL\_TEND}

# Appendix C: Evaluation of threats

${TABLE\_THREATS\_FULL}

# Appendix D: Asset context

${TABLE\_ASSET\_CONTEXT}

# Appendix E: Risk owners

${TABLE\_RISK\_OWNERS}

# Appendix F: Notes and comments from the consultant

## Information risks

${TABLE\_AUDIT\_INSTANCES}

## Operational risks

${TABLE\_AUDIT\_RISKS\_OP}