****

**${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}

Contents

[1 Introduction 3](#_Toc75419076)

[1.1 Placing the risk analysis in context 3](#_Toc75419077)

[1.2 Aims of the document 3](#_Toc75419078)

[1.3 Acronyms/Glossary 3](#_Toc75419079)

[2 Context Establishment 4](#_Toc75419080)

[2.1 Description of the context 4](#_Toc75419081)

[2.2 Definition of the risk evaluation criteria 4](#_Toc75419082)

[2.2.1 Information risks 4](#_Toc75419083)

[2.2.1.1 Impact scale 4](#_Toc75419084)

[2.2.1.2 Threat scale 4](#_Toc75419085)

[2.2.1.3 Vulnerability scale 4](#_Toc75419086)

[2.2.1.4 Risk acceptance thresholds 5](#_Toc75419087)

[2.2.2 Operational risks 5](#_Toc75419088)

[2.2.2.1 Impact scale 5](#_Toc75419089)

[2.2.2.2 Likelihood scale 5](#_Toc75419090)

[2.2.2.3 Risk acceptance thresholds 5](#_Toc75419091)

[2.3 Evaluation of trends and threats 5](#_Toc75419092)

[Appendix A: Interview and information collection 6](#_Toc75419093)

[Appendix B: Evaluation of trends 7](#_Toc75419094)

[Appendix C: Evaluation of threats 8](#_Toc75419095)

**Read and approved by all the parties**

# Introduction

## Placing the risk analysis in context

${CONTEXT\_ANA\_RISK}

## Aims of the document

This document has the goal to show the risks context, as understood and transposed by the responsible for the risk management.

This document has to be signed, for reading and acceptance by the management of the target organisation to allow the continuing of the mission.

## 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.

# 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}

# Appendix A: Interview and information collection

${TABLE\_INTERVIEW}

# Appendix B: Evaluation of trends

${TABLE\_EVAL\_TEND}

# Appendix C: Evaluation of threats

${TABLE\_THREATS\_FULL}