Appendix 3 – Risk Assessment and Treatment Report

Commented [270011]: To learn how to fill out this document, and to see real-life examples of what you need to write, watch this video tutorial: "How to Write ISO 27001 Risk Assessment Report".

To access the tutorial: In your Inbox, find the email that you received at the moment of purchase. There, you will see a link and a password that will enable you to access the video tutorial.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. Purpose, scope and users

The purpose of this document is to give a detailed overview of the process and documents used during risk assessment and treatment of disruptive risks in [organization name] in the period [specify period].

Risk assessment was applied to the entire Information Security Management System (ISMS).

This document is intended for top management of [organization name], [job title responsible for information security], owners of information assets, and everyone involved in planning, implementing, monitoring and improving the ISMS.

Commented [270012]: Insert the name of your organization.

Commented [270013]: Insert the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clauses 8.2 and 8.3
- ISO 22301 standard, clause 8.2.3
- ISMS Scope
- Information Security Policy
- Business Continuity Policy
- Risk Assessment and Risk Treatment Methodology

Commented [270014]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "04_ISMS_Scope".

Commented [27A5]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "05_General_Policies".

Commented [27A6]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "10_ISO_22301_Core_Business_Continuity_Documents".

3. Process of assessment and treatment of information risks

The entire risk assessment and risk treatment process has been carried out according to the Risk Assessment and Risk Treatment Methodology document.

3.1. Purpose of risk management

[illegible]
criticality of individual risks.

The purpose of risk treatment is to define systematic means of reducing or controlling such risks.

3.2. Risk assessment and risk treatment scope

[illegible]
with the ISMS Scope document.

Commented [270017]: Include only the organizational units where the risk assessment and risk treatment were performed.

3.3. Time period

[illegible]
prepared during [specify period].

3.4. Participants in the process and collection of information

[redacted]

During risk assessment, information was collected through questionnaires and interviews with responsible persons, i.e. asset owners from all organizational units.

Commented [270018]: E.g.: Business continuity manager, Security manager, Information Security Manager, etc.

Commented [270019]: You can delete this part if no expert assistance was used.

Commented [2700110]: Or describe some other method if used.

3.5. Brief overview of the applied methodology

Briefly, the process was conducted in the following way:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- the level of risk was calculated by adding up consequence and likelihood
- risks valued 3 and 4 were determined as unacceptable risks
- [redacted]
- [redacted]

Commented [2700111]: Delete this text if only the controls from Annex A of the ISO/IEC 27001 were applied.

3.6. Overview of documents used during the risk assessment and risk treatment process

The following documents were used or drawn up during the implementation of risk assessment and risk treatment:

- [redacted]
- [redacted]

4. Validity and document management

This document is valid as of [date]. Owner of this document is [job title].

Commented [2700112]: E.g.: Business continuity manager, Security manager, Information Security Manager, etc.

5. Appendices

- [redacted]
- [redacted]

[job title]
[name]

_____
[signature]

Commented [2700113]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.