Appendix 3 – Risk Assessment and Treatment Report

Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>27001Academy</td>
<td>Basic document outline</td>
<td></td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS .........................................................................................2
2. REFERENCE DOCUMENTS ................................................................................................2
3. PROCESS OF ASSESSMENT AND TREATMENT OF INFORMATION RISKS .........................2
   3.1. PURPOSE OF RISK MANAGEMENT ........................................................................ 2
   3.2. RISK ASSESSMENT AND RISK TREATMENT SCOPE ...................................... 2
   3.3. TIME PERIOD ................................................................................................... 2
   3.4. PARTICIPANTS IN THE PROCESS AND COLLECTION OF INFORMATION .......... 3
   3.5. BRIEF OVERVIEW OF THE APPLIED METHODOLOGY ................................... 3
   3.6. OVERVIEW OF DOCUMENTS USED DURING THE RISK ASSESSMENT AND RISK TREATMENT PROCESS ................................................................. 3
4. VALIDITY AND DOCUMENT MANAGEMENT ..................................................................3
5. APPENDICES ..................................................................................................................3
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.

2. Reference documents

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

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

The purpose of risk management is to identify risks, their consequences, and evaluate their criticality to the organization. The assessment results are documented in the Risk Management Plan, which forms part of the ISMS.

3.2. Risk assessment and risk treatment scope

Risk assessment and risk treatment was carried out in [name of organizational units], in accordance with the [specify procedures].

3.3. Time period

The final report was prepared during [specify period].

Appendix 3 – Risk Assessment and Treatment Report

©2020 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.
3.4. Participants in the process and collection of information

The risk assessment and risk treatment processes were managed by [name and job title], with expert support from [expert support names]. The process was carried out in two phases: identification of external assets and identification of risks. Suitable experts were identified to carry out the process and the assets were identified in an initial workshop. The process was conducted with the participation of responsible persons, i.e. asset owners from all organizational units.

3.5. Brief overview of the applied methodology

Briefly, the process was conducted in the following way:

- The risk assessment and risk treatment processes were managed by [name and job title], with expert support from [expert support names].
- The process was carried out in two phases: identification of external assets and identification of risks.
- Suitable experts were identified to carry out the process and the assets were identified in an initial workshop.
- The process was conducted with the participation of responsible persons, i.e. asset owners from all organizational units.
- The likelihood of risk occurrence, i.e. that the threat will exploit the vulnerability, was evaluated using values 0 to 2.
- After controls were applied, residual risks were assessed.

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:

- [List of documents]

4. Validity and document management

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

5. Appendices

- Appendix 1 – Risk Assessment Table
- Appendix 2 – Risk Treatment Table