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 ................................................ 2
   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

©2020 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.
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 information 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
- ISMS Scope Document
- Information Security 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 assessment is to identify all assets, their vulnerabilities, and threats that could

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 ISMS Scope document.

3.3. Time period

The report was prepared on [date] based on risk assessment and risk treatment that was prepared during [specify period].

3.4. Participants in the process and collection of information
The risk assessment and risk treatment process was managed by [name and job title], with expert
[Commented [27A5]: E.g.: Business continuity manager, Security manager, Information Security Manager, etc.]
[Commented [27A6]: You can delete this part if no expert assistance was used.]
[Commented [27A7]: Or describe some other method if used.]

3.5. Brief overview of the applied methodology

Briefly, the process was conducted in the following way:

- values 0 to 2
- the likelihood of risk occurrence, i.e. that the threat will exploit the vulnerability, was
- reduce the risk to an acceptable level were selected from Annex A of the ISO/IEC 27001 standard, as well as from other security control sources deemed relevant

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

The following documents were used to document and manage the implementation of the assessment and

treatment of identified risks.

- Risk Assessment Table (Appendix 1) – for each combination of assets, vulnerabilities and threats, this table shows the values for consequence and likelihood, and calculates the risk

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

[job title]
[name]

[signature]

Commented [27A10]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.