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>EUGDPRAcademy</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

Commented [EU GDPR1]: 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, choose one of the following options (depending on how you received the document):

a) For document(s) delivered via Conformio: log into Conformio, click “Helpful materials” in the top menu, choose your language, and open the folder “Video tutorials.”

b) For document(s) delivered via email: In your inbox, find the email that you received at the moment of purchase – there, you will see a link that will enable you to access the video tutorial.
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 cause damage or loss of information or harm to business operations in order to minimize the impact and potential losses.

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

3.2. Risk assessment and risk treatment scope

Risk assessment and risk treatment was carried out in terms of organizational assets, in accordance with the ISMS scope document.

3.3. Time period

Risk assessment was implemented in the period from [day/month/year] to [day/month/year]. Risk treatment was implemented in the period from [day/month/year] to [day/month/year].

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 assistance provided by [If expert assistance was used, provide name and company].

3.5. Brief overview of the applied methodology

Briefly, the process was conducted in the following way:

- all assets were identified, as well as their owners
- the process was conducted using [methodology]
- the likelihood of risk occurrence, i.e. that the threat will exploit the vulnerability, was evaluated using values 0 to 2
- the level of risk was calculated by adding up consequence and likelihood

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:

- Risk Assessment Table (Appendix 1) – for each combination of assets, vulnerabilities and threats:
  - [description]

4. Validity and document management

This document is valid as of [date]. Issue of this document is [date today]

5. Appendices

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