RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY

Code: 

Version: 

Date of version: 

Created by: 

Approved by: 

Confidentiality level: 

©2019 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.
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></td>
<td>0.1</td>
<td>27001Academy</td>
<td>Basic document outline</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS ................................................................................................................. 3
2. REFERENCE DOCUMENTS.......................................................................................................................... 3
3. RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY ............................................................................ 3
   3.1. RISK ASSESSMENT ............................................................................................................................... 3
       3.1.1. The process.................................................................................................................................... 3
       3.1.2. Assets, vulnerabilities and threats ................................................................................................. 3
       3.1.3. Determining the risk owners ......................................................................................................... 3
       3.1.4. Consequences and likelihood ....................................................................................................... 4
   3.2. RISK ACCEPTANCE CRITERIA ............................................................................................................... 4
   3.3. RISK TREATMENT ............................................................................................................................... 4
   3.4. REGULAR REVIEWS OF RISK ASSESSMENT AND RISK TREATMENT ............................................. 5
   3.5. STATEMENT OF APPLICABILITY AND RISK TREATMENT PLAN .................................................... 5
   3.6. REPORTING ........................................................................................................................................ 5
4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT ........................................................... 5
5. VALIDITY AND DOCUMENT MANAGEMENT ........................................................................................... 6
6. APPENDICES ............................................................................................................................................. 7
1. Purpose, scope and users

The purpose of this document is to define the methodology for assessment and treatment of information risks in [organization name], and to define the acceptable level of risk according to the ISO/IEC 27001 standard.

Risk assessment and risk treatment are applied to the entire scope of the Information Security Management System (ISMS), i.e. to all assets which are used within the organization or which could have an impact on information security within the ISMS.

Users of this document are all employees of [organization name] who take part in risk assessment and risk treatment.

2. Reference documents

- ISO/IEC 27001 standard, clauses 6.1.2, 6.1.3, 8.2, and 8.3
- ISO 22301 standard clauses 8.1.2 and 8.2.3
- Information Security Policy
- List of Legal, Regulatory and Contractual and Other Requirements
- Supplier Security Policy
- Statement of Applicability

3. Risk Assessment and Risk Treatment Methodology

3.1. Risk assessment

3.1.1. The process

Risk assessment is implemented through the Risk Assessment Table. The risk assessment process is...

3.1.2. Assets, vulnerabilities and threats

The first step in risk assessment is the identification of all assets in the ISMS scope – i.e. of all assets, equipment, infrastructure, and external services/outsource services. When identifying assets, it is also necessary to identify their owners – the person or organizational unit responsible for each asset...

3.1.3. Determining the risk owners

Commented [27AS]: Write “ISO 22301 standard” if you are implementing only ISO 22301 and not ISO 27001.
Commented [27A6]: Write only “Business Continuity Management System / BCM” if you are implementing only ISO 22301.
Commented [27A7]: Same as previous comment.

Commented [27AB]: Delete this if you are implementing only ISO 22301.
Commented [27A9]: Delete this if you are implementing only ISO 27001.
Commented [27A10]: Delete this if you are implementing only ISO 22301.
Commented [27A11]: Delete if you won’t be using this policy.
Commented [27A12]: Delete this if you are implementing only ISO 22301.

Commented [27A13]: This Methodology must be amended if so required by legal and regulatory requirements or contractual obligations.

Commented [27A14]: To simplify the process, you can define that asset owner for each risk will also be the risk owner.

To improve the risk awareness of the asset owners you can use this security awareness training:
https://training.adviser.com/awareness-session/security-awareness-training/

Commented [27A15]: Add also other types of assets not included in this list.
3.1.4. **Consequences and likelihood**

Once risk owners have been identified, it is necessary to assess consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes:

<table>
<thead>
<tr>
<th>Low consequence</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate consequence</td>
<td>1</td>
</tr>
<tr>
<td>High consequence</td>
<td>2</td>
</tr>
</tbody>
</table>

After the assessment of consequences, it is necessary to assess the likelihood of occurrence of such a risk, i.e. the probability that a threat will exploit the vulnerability of the respective asset:

<table>
<thead>
<tr>
<th>Low likelihood</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate likelihood</td>
<td>1</td>
</tr>
<tr>
<td>High likelihood</td>
<td>2</td>
</tr>
</tbody>
</table>

By entering the values of consequence and likelihood into the Risk Assessment Table, the level of risk can be determined.

3.2. **Risk acceptance criteria**

Values 0, 1 and 2 are acceptable risks, while values 3 and 4 are unacceptable risks. Unacceptable risks must be treated.

3.3. **Risk treatment**
1. Selection of security control or controls from Annex A of the ISO/IEC 27001 standard or some other security controls

2.

3.

4.

The selection of options is implemented through the Risk Treatment Table. Usually, option 1 is selected: selection of one or more security controls. When several security controls are selected for a risk, then additional rows are inserted into the table immediately below the row specifying the risk.

planned controls.

3.4. Regular reviews of risk assessment and risk treatment

Risk owners must review existing risks and update the Risk Assessment Table and Risk Treatment Table in line with newly identified risks. The review is conducted at least once a year, or more

3.5. Statement of Applicability and Risk treatment plan

[Job title] must document the following in the Statement of Applicability: which security controls

[Job title] will prepare the Risk treatment plan in which the implementation of controls will be planned. On behalf of the risk owners, [top management] will approve the Risk treatment plan.

3.6. Reporting

[Job title] will document the results of risk assessment and risk treatment, and all of the subsequent

4. Managing records kept on the basis of this document

<table>
<thead>
<tr>
<th>Record name</th>
<th>Storage location</th>
<th>Person</th>
<th>Control for record</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment and Risk Treatment Methodology</td>
<td>ver [version] from [date]</td>
<td></td>
<td></td>
<td>Page 9 of 7</td>
</tr>
</tbody>
</table>

©2019 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.
<table>
<thead>
<tr>
<th>[organization name]</th>
<th>[confidentiality level]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Assessment Table (electronic form – Excel document)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[job title]’s computer</td>
</tr>
<tr>
<td><strong>Risk Treatment Table (electronic form – Excel document)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[job title]’s computer</td>
</tr>
<tr>
<td><strong>Risk Assessment and Treatment Report (electronic form – PDF format)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[job title]’s computer</td>
</tr>
<tr>
<td><strong>Statement of Applicability (electronic form – PDF format)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[job title]’s computer</td>
</tr>
<tr>
<td><strong>Risk Treatment Plan (electronic form – Word document)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[job title]’s computer</td>
</tr>
</tbody>
</table>

Only [job title] can grant other employees access to any of the abovementioned documents.

5. **Validity and document management**

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year, before the regular review of existing risk assessment.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

Commented [27A22]: Insert the data in this column to reflect your real needs.

Commented [27A23]: Delete this if you are implementing only ISO 22301.

Commented [27A24]: This is only a recommendation; adjust frequency as appropriate.
6. Appendices
   
   - Appendix 1 – Risk Assessment Table
   - Appendix 2 – Risk Treatment Table
   - Appendix 3 – Risk Assessment and Treatment Report

[signature]