[organization logo]

[organization name]

**RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415649007)

[2. Reference documents 3](#_Toc415649008)

[3. Risk Assessment and Risk Treatment Methodology 3](#_Toc415649009)

[3.1. Risk assessment 3](#_Toc415649010)

[3.1.1. The process 3](#_Toc415649011)

[3.1.2. Assets, vulnerabilities and threats 3](#_Toc415649012)

[3.1.3. Determining the risk owners 3](#_Toc415649013)

[3.1.4. Consequences and likelihood 4](#_Toc415649014)

[3.2. Risk acceptance criteria 4](#_Toc415649015)

[3.3. Risk treatment 4](#_Toc415649016)

[3.4. Regular reviews of risk assessment and risk treatment 5](#_Toc415649017)

[3.5. Statement of Applicability and Risk treatment plan 5](#_Toc415649018)

[3.6. Reporting 5](#_Toc415649019)

[4. Managing records kept on the basis of this document 5](#_Toc415649020)

[5. Validity and document management 6](#_Toc415649021)

[6. Appendices 7](#_Toc415649022)

# 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.

# Reference documents

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

# Risk Assessment and Risk Treatment Methodology

## Risk assessment

### The process

Risk assessment is implemented through the Risk Assessment Table. The risk assessment process is coordinated by [job title], identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and likelihood is performed by risk owners.

### 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 which may affect confidentiality, integrity and availability of information in the organization. Assets may include documents in paper or electronic form, applications and databases, people, IT equipment, infrastructure, and external services/outsourced processes. When identifying assets, it is also necessary to identify their owners – the person or organizational unit responsible for each asset.

The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities are identified using the catalogues included in the Risk Assessment Table. Every asset may be associated with several threats, and every threat may be associated with several vulnerabilities.

### Determining the risk owners

For each risk, a risk owner has to be identified – the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner.

### 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:

|  |  |  |
| --- | --- | --- |
| Low consequence | 0 | Loss of confidentiality, availability or integrity does not affect the organization's cash flow, legal or contractual obligations, or its reputation. |
| Moderate consequence | 1 | Loss of confidentiality, availability or integrity incurs costs and has a low or moderate impact on legal or contractual obligations, or the organization's reputation. |
| High consequence | 2 | Loss of confidentiality, availability or integrity has considerable and/or immediate impact on the organization's cash flow, operations, legal or contractual obligations, or its reputation. |

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:

|  |  |  |
| --- | --- | --- |
| Low likelihood | 0 | Existing security controls are strong and have so far provided an adequate level of protection. No new incidents are expected in the future. |
| Moderate likelihood | 1 | Existing security controls are moderate and have mostly provided an adequate level of protection. New incidents are possible, but not highly likely. |
| High likelihood | 2 | Existing security controls are low or ineffective. Such incidents have a high likelihood of occurring in the future. |

By entering the values of consequence and likelihood into the Risk Assessment Table, the level of risk is calculated automatically by adding up the two values. Existing security controls are to be entered in the last column of the Risk Assessment Table.

## Risk acceptance criteria

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

## Risk treatment

Risk treatment is implemented through the Risk Treatment Table, by copying all risks identified as unacceptable from the Risk Assessment Table. Risk treatment is conducted by [job title].

One or more treatment options must be selected for risks valued 3 and 4:

1. Selection of security control or controls from Annex A of the ISO/IEC 27001 standard or some other security controls
2. Transferring the risks to a third party – e.g. by purchasing an insurance policy or signing a contract with suppliers or partners
3. Avoiding the risk by discontinuing a business activity that causes such risk
4. Accepting the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialize

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.

The treatment of risks related to outsourced processes must be addressed through the contracts with responsible third parties, as specified in [Supplier Security Policy].

In the case of option 1 (selection of security controls), it is necessary to assess the new value of consequence and likelihood in the Risk Treatment Table, in order to evaluate the effectiveness of planned controls.

## 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 frequently in the case of significant organizational changes, significant change in technology, change of business objectives, changes in the business environment, etc.

## Statement of Applicability and Risk treatment plan

[job title] must document the following in the Statement of Applicability: which security controls from Annex A of the ISO/IEC 27001 standard are applicable and which are not, the justification for such decisions, and whether they are implemented or not.

On behalf of the risk owners, [top management] will accept all residual risks through the Statement of Applicability.

[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.

## Reporting

[job title] will document the results of risk assessment and risk treatment, and all of the subsequent reviews, in the Risk Assessment and Treatment Report.

[job title] will monitor the progress of implementation of the Risk treatment plan and report the results to [job title] each month.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Control for record protection | Retention time |
| Risk Assessment Table (electronic form – Excel document) | [job title]'s computer | [job title of the owner of the Risk Assessment Table] | Only [job title] has the right to make entries into and changes to the Risk Assessment Table. | Data is stored permanently. |
| Risk Treatment Table (electronic form – Excel document) | [job title]'s computer | [job title of the owner of the Risk Treatment Table] | Only [job title] has the right to make entries into and changes to the Risk Treatment Table. | Data is stored permanently. |
| Risk Assessment and Treatment Report (electronic form – PDF format) | [job title]'s computer | [job title of the owner of the Report] | The Report is prepared in read-only PDF format | The Report is stored for a period of 3 years |
| Statement of Applicability (electronic form – PDF format) | [job title]'s computer | [job title of the owner of the Report] | Only [job title] has the right to make entries into and changes to the Statement of Applicability | Older versions of SoA are stored for a period of 3 years |
| Risk treatment plan (electronic form – Word document) | [job title]'s computer | [job title of the person responsible for the Risk treatment plan] | Only [job title] has the right to make entries into and changes to the Risk treatment plan | Older versions of Risk treatment plan are stored for a period of 3 years |

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

# 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:

* the number of incidents which occurred, but were not included in risk assessment
* the number of risks which were not treated adequately
* the number of errors in the risk assessment and risk treatment process because of unclear definition of roles and responsibilities

# Appendices

* Appendix 1: Form – Risk Assessment Table
* Appendix 2: Form – Risk Treatment Table
* Appendix 3: Form – Risk Assessment and Treatment Report

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]