\*\* FREE PREVIEW VERSION \*\*

[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** |
| 01/10/2013 | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc368671208)

[2. Reference documents 3](#_Toc368671209)

[3. Risk Assessment and Risk Treatment Methodology 3](#_Toc368671210)

[3.1. Risk assessment 3](#_Toc368671211)

[3.1.1. The process 3](#_Toc368671212)

[3.1.2. Assets, vulnerabilities and threats 3](#_Toc368671213)

[3.1.3. Determining the risk owners 3](#_Toc368671214)

[3.1.4. Consequences and likelihood 4](#_Toc368671215)

[3.2. Risk acceptance criteria 4](#_Toc368671216)

[3.3. Risk treatment 4](#_Toc368671217)

[3.4. Regular reviews of risk assessment and risk treatment 5](#_Toc368671218)

[3.5. Statement of Applicability and Risk treatment plan 5](#_Toc368671219)

[3.6. Reporting 5](#_Toc368671220)

[4. Managing records kept on the basis of this document 5](#_Toc368671221)

[5. Validity and document management 6](#_Toc368671222)

[6. Appendices 7](#_Toc368671223)

# 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.

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <http://www.iso27001standard.com/en/documentation/Risk-Assessment-and-Risk-Treatment-Methodology>