\*\* FREE PREVIEW VERSION \*\*

Thank you for downloading the free preview version of the ISO 27001 Documentation Toolkit.

If you have decided that the ISO 27001 Documentation Toolkit is the right choice for your company, please see the table below to choose the toolkit with the required expert support level.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Toolkit with expert support** | **Toolkit with extended support** | **Power toolkit** |
|  | **US $897** | **US $1397** | **US $2397** |
| **45 document templates compliant with ISO 27001** |  |  |  |
| **Access to video tutorials** |  |  |  |
| **Email support** | 10 questions per month | Unlimited | Unlimited |
| **One-on-one support with an ISO 27001 expert** | 1 hour | 5 hours | 15 hours |
| **Expert review (completed documents)** | 1 document | 5 documents | 15 documents |
| **Pre-audit check** | **X** |  |  |
|  | [**BUY NOW**](https://shop.advisera.com/order/checkout.php?PRODS=4717085&QTY=1&CART=1&CARD=1?utm_source=Toolkit%20Document%20Preview&utm_medium=downloaded-content&utm_campaign=ISO%2027001%20templates&utm_term=Toolkit%20with%20expert%20support&utm_content=lang-en) | [**BUY NOW**](https://shop.advisera.com/order/checkout.php?PRODS=4718147&QTY=1&CART=1&CARD=1?utm_source=Toolkit%20Document%20Preview&utm_medium=downloaded-content&utm_campaign=ISO%2027001%20templates&utm_term=Toolkit%20with%20extended%20support&utm_content=lang-en) | [**BUY NOW**](https://shop.advisera.com/order/checkout.php?PRODS=4717086&QTY=1&CART=1&CARD=1?utm_source=Toolkit%20Document%20Preview&utm_medium=downloaded-content&utm_campaign=ISO%2027001%20templates&utm_term=Toolkit%20with%20power%20support&utm_content=lang-en) |
|  | (click the link above using CTRL+click) | | |

[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** |
|  | 0.1 | 27001Academy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc105589247)

[2. Reference documents 3](#_Toc105589248)

[3. Risk Assessment and Risk Treatment Methodology 3](#_Toc105589249)

[3.1. Risk assessment 3](#_Toc105589250)

[3.1.1. The process 3](#_Toc105589251)

[3.1.2. Assets, vulnerabilities and threats 3](#_Toc105589252)

[3.1.3. Determining the risk owners 4](#_Toc105589253)

[3.1.4. Consequences and likelihood 4](#_Toc105589254)

[3.2. Risk acceptance criteria 4](#_Toc105589255)

[3.3. Risk treatment 4](#_Toc105589256)

[3.4. Regular reviews of risk assessment and risk treatment 5](#_Toc105589257)

[3.5. Statement of Applicability and Risk Treatment Plan 5](#_Toc105589258)

[3.6. Reporting 5](#_Toc105589259)

[4. Managing records kept on the basis of this document 5](#_Toc105589260)

[5. Validity and document management 6](#_Toc105589261)

[6. Appendices 7](#_Toc105589262)

# 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, 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. [Job title] is responsible for including the data about threats, vulnerabilities, consequences, and likelihood in the Risk Assessment Table.

### Assets, vulnerabilities and threats

…

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

To download full version of this document click here:  
<https://advisera.com/27001academy/documentation/risk-assessment-and-risk-treatment-methodology/>