[Organization logo]

[Organization name]

RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY

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

Commented [270012]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [270013]: To learn how to write the methodology, read these articles:

- ISO 27001 risk assessment & treatment – six main steps https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#section2
- How to write ISO 27001 risk assessment methodology https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#section3

Commented [270014]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

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.

Commented [270015]: Write "ISO 22301 standard" if you are implementing only ISO 22301 and not ISO 27001.

Commented [270016]: Write only "Business Continuity Management System (BCMS)" if you are implementing only ISO 22301.

Commented [270017]: Same as previous comment.

Commented [270018]: Include the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clauses 6.1.2, 6.1.3, 8.2, and 8.3
- ISO 22301 standard clauses 8.2.1, 8.2.3 and 8.3.2
- Information Security Policy
- List of Legal, Regulatory, Contractual, and Other Requirements
- Supplier Security Policy
- Statement of Applicability

Commented [270019]: Delete this if you are implementing only ISO 22301.

Commented [2700110]: Delete this if you are implementing only ISO 27001.

Commented [2700111]: Delete this if you are implementing only ISO 22301.

Commented [2700112]: Delete if you won't be using this policy.

Commented [2700113]: Delete this if you are implementing only ISO 22301.

3. Risk Assessment and Risk Treatment Methodology

Commented [2700114]: [illegible]

3.1. Risk assessment

3.1.1. The process

[illegible] for including the data about threats, vulnerabilities, consequences, and likelihood in the Risk Assessment Table.

Commented [2700115]: 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.advisera.com/awareness-session/security-awareness-training/

3.1.2. Assets, vulnerabilities and threats

The first step in risk assessment is the identification of all assets in the ISMS scope by the [illegible] organizational unit responsible for each asset.

Commented [2700116]: Add also other types of assets not included in this list.

The next step is for the asset owners to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities are identified using the catalogues included in the Risk Assessment [illegible] several vulnerabilities.

3.1.3. *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.

Commented [2700117]: To simplify the process, you can define that asset owner for each risk will also be the risk owner.

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:

Low consequence	0	Loss of confidentiality, availability or integrity does not affect the organization's cash flow, legal or contractual obligations, or its reputation.
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

[illegible] 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.
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

By entering the values of consequence and likelihood into the Risk Assessment Table, the level of risk [illegible]

3.2. Risk acceptance criteria

Risks with levels 0, 1, and 2 are acceptable risks, while risks with levels 3 and 4 are unacceptable risks. Unacceptable risks must be treated.

3.3. Risk treatment

[illegible] unacceptable from the Risk Assessment Table. Risk treatment is conducted by [job title].

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

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible] options would cost more than the potential impact should such risk materialize

[illegible]

[illegible] 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.

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 [illegible] of business objectives, changes in the business environment, etc.

3.5. Statement of Applicability and Risk Treatment Plan

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

[illegible]

[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 [illegible]

[illegible] results to [job title] each month.

Commented [2700118]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700119]: E.g.: ISO 27001 standard Annex A controls, NIST Special Publications, etc.

Note: The Risk Treatment Table template supports ISO 27001 standard Annex A controls.

Commented [2700120]: [illegible]

Commented [2700121]: Delete this if you will not be using this policy.

Commented [2700122]: This new value is called "Residual Risk".

Commented [2700123]: Delete this if you are implementing only ISO 22301.

Commented [2700124]: [illegible]

Commented [2700125]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "08_Implementation_Plan".

Commented [2700126]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700127]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700128]: E.g.: CEO, responsible for the business unit, etc.

Commented [2700129]: This is only a recommendation. Please assess whether this frequency is appropriate to your company practices and modify if needed.

4. 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

[illegible]

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.

Commented [2700130]: Insert the data in this column to reflect your real needs.

Commented [2700131]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700132]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700133]: Delete this if you are implementing only ISO 22301.

Commented [2700134]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700135]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700136]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]
- [illegible]
- [illegible] definition of roles and responsibilities

6. Appendices

- [illegible]
- [illegible]
- [illegible]

[job title]
[name]

____
[signature]

Commented [2700137]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.