**Risk Assessment and Risk Treatment Report**

Version:

Date:

Classification

Document Control

|  |  |  |
| --- | --- | --- |
| 1. | Document Number: |  |
| 2. | Version History: |  |
| 3. | Created Date: |  |
| 4. | Created By: |  |
| 5. | Approved By: |  |
| 6. | Contact: |  |

Document Modify History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modified By | Modification |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Objectives, Focus Area and Usable Parties 4](#_Toc179679163)

[Reference Documents 4](#_Toc179679164)

[Process of Treatment and Assessment of Information Risks 5](#_Toc179679165)

[Risk Assessment and Treatment Methodology 6](#_Toc179679166)

[I. Risk Assessment 6](#_Toc179679167)

[II. Risk Acceptance 6](#_Toc179679168)

[III. Risk Treatment 7](#_Toc179679169)

[IV. Regular Feedback on Risk Assessment and Risk Treatment 7](#_Toc179679170)

[V. Statement of Applicability and Risk Treatment Plan 7](#_Toc179679171)

[VI. Reporting 8](#_Toc179679172)

[Mining Control of records based on this document 8](#_Toc179679173)

[Validity and Document Management 9](#_Toc179679174)

# Objectives, Focus Area and Usable Parties

**Objectives:**

The purpose of this paper is to offer a comprehensive analysis of the documentation and methodology utilized by [name of organization] for the purpose of evaluating and managing information risks within the period of time that has been specified. It provides a description of the process by which [business name] evaluates and manages information risks in line with the ISO/IEC 27001 standard, including the determination of an acceptable risk level.

**Focus Area:**

This document is subject to the entire ISMS documentation. The scope includes all the resources utilized by the company and any factors that could impact information security within the Information Security Management System (ISMS), representing its complete range. This comprehensive approach also includes the evaluation and management of related risks.

**Usable Parties:**

The top management of [organization name], those with [job title], asset owners, and everyone involved in the planning, supervision, and implementation of the ISMS would all benefit from this paper. It is applicable to every employee at [name of organization].

# Reference Documents

* ISO 27001 Standards, Clause 6.1.2, 6.13, 8.2, 8.3
* ISMS Scope Document
* Information Security Policy
* Risk assessment and Treatment Methodology
* List of legislation and contractual requirements document

# Process of Treatment and Assessment of Information Risks

1. **Purpose of managing risks:**

Risk assessment is used to find all assets, identify their vulnerabilities, and recognize possible threats that could take advantage of these weaknesses. Also, it includes a detailed look at these attributes to evaluate how serious certain threats are.

1. **Risks Assessment and Treatment Scope:**

This document is subject to the entire ISMS documentation. The scope includes all the resources utilized by the company and any factors that could impact information security within the Information Security Management System (ISMS), covering its complete range. This comprehensive approach also includes the evaluation and management of related risks.

1. **Tine Period:**

The time period specifies when the risk assessment and treatment take place, and it also indicates how frequently the organization should conduct risk assessments and treatment plans. For example, every month.

1. **Participants of the process and Information:**

This identifies the parties involved in risk assessments and treatments, as well as the primary accountable parties and authorized personnel in charge of carrying out risk assessment duties inside the [organization name].

# Risk Assessment and Treatment Methodology

## Risk Assessment

* **Process:**

The Risk Assessment Table is used to carry out risk assessments. The risk assessment process is overseen by [job title]. Asset owners are responsible for identifying risks and vulnerabilities, while risk owners evaluate the potential impacts and the likelihood of those risks happening.

* **Asset, Threats, and Vulnerabilities:**

Identifying potential risks and weaknesses in the company's assets is the initial step in the risk assessment process. The company needs to identify the risks and associated vulnerabilities for each asset in order to categorize these threats and vulnerabilities effectively.

* **Choosing the Risk Owner:**

A person who has the authority to manage risks is referred to as a risk owner. The organization should select individuals who are closely involved with the relevant processes and operations where risks have been identified when appointing risk owners. It’s important that these individuals are the ones who are directly impacted by the risks and would face the consequences if those risks actually happened.

* **Likelihood and Consequence:**

Every risk should be separately examined for its impact and likelihood by the [job title]. The [job title] is free to choose the scale that best suits their needs. as in medium, high, and low.

## Risk Acceptance

Risk can be seen as acceptable if the risk assessment calculation results in values ranging from 2 to 10. If a risk is rated a 7, it indicates that only potential risks rated 8, 9, and 10 need special attention. Instead of just relying on set numerical criteria, we can look at each risk individually, using expertise and experience to guide our evaluation.

## Risk Treatment

There are four methods to manage each unacceptable risk:

1. Implement a security measure outlined in Annex A.
2. shift the risk to a third party
3. Make behavioral changes to reduce the risk, such as substituting safer activities for risky ones.
4. Acknowledge and accept the risk, particularly if reducing it would be too expensive.

## Regular Feedback on Risk Assessment and Risk Treatment

* **Staff Engagement and Awareness:**

Provide a forum for providing and receiving feedback, and involve the relevant staff in the process on a regular basis.

* **Management Reviews:**

The Management Review's goal is to verify that, given the organization's mission, challenges, and information asset risks, the ISMS and its goals remain appropriate, acceptable, and successful. There must be a management review at least once a year. It is recommended that risk owners regularly review their risk assessment.

* **Improvement:**

Internal audits can be helpfully included into the more extensive strategic risk assessment processes, as can the employment of the other techniques listed in clause 10 for improvement.

## Statement of Applicability and Risk Treatment Plan

Clearly and concisely outline the organization's internal implementation of the risk treatment plan. Describe the chosen controls and the rationale for their application in lowering the identified risks. Indicate if you have put these controls in place or not. Justify the decision to leave controls out of ISO Annex A.

## Reporting

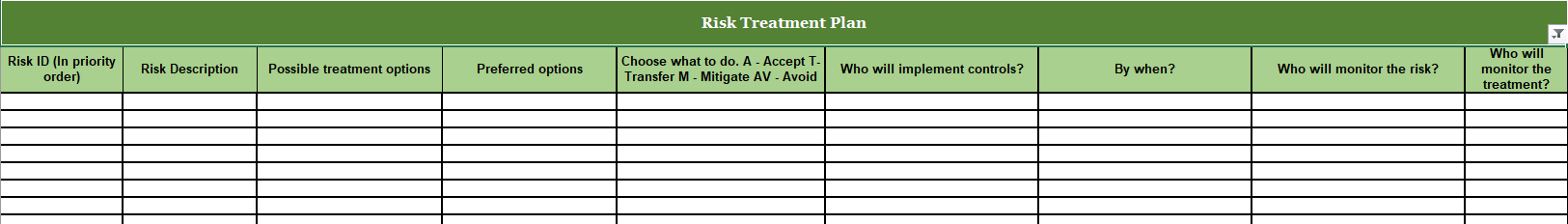
The reporter must mention all the details of risks and what the organization have done so far.

* **Risk Assessment Table:**

A close-up of a screen

Description automatically generated

* **Risk Treatment Plan:**



# Mining Control of records based on this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of the record | Storage Location | Responsible person for storage | Controls for record protection | Retention time |
|  |  |  |  |  |
|  |  |  |  |  |

# Validity and Document Management

The document's validity commences on: [date]

As the owner of this document, [job title] bears the responsibility of conducting periodic checks and making necessary updates, with a minimum frequency of once a year.

When executing this procedure, the following criteria must be adhered to:

* The guidelines provided in this page must be followed while creating any document.
* Each document must go through a regulated procedure in order to be created, approved, distributed, used, and updated.

[Job Title]

[Name]

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

[Signature]