Risk Management, Assessment, and Treatment Policy

|  |  |
| --- | --- |
| Owner |  |
| Approver |  |
| Last Reviewed |  |

## Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| GRC | Performance and Maintenance of Risk Management Process |
| Leadership Team | Risk Identification, Risk Mitigation, Risk approval |
| CFO | Senior Management Approval |

Further roles and responsibilities may be added to the above table as the risk assessment and treatment process matures within [Company Name].

## The Risk assessment and treatment process

The process described in this document is aligned with the following international standards:  ISO/IEC 27001  Information Security Management Systems

This document shall be reviewed annually for approval. The risk process is qualitative in nature in that it uses the terms high, medium and low to describe the relative classification level for each specific risk. In all cases where quantitative techniques are used the criteria should be clearly stated so that the risk assessment is understandable and repeatable.

## Criteria for performing information security risk assessments

A risk assessment will be performed in the following circumstances:

 An annual risk assessment covering the enterprise, including information assets as part of the initial implementation of the Information Security Management System ISMS

 Projects that involve significant change to the risk management methodology, organization, ISMS, information assets, or major external changes (i.e. regulatory, M&A

 Vendors shall be assessed for risk as part of the vendor management process

## Risk Assessment Methodology Establish scope and context

The overall environment in which the risk assessment is carried out shall be described and the reasons for it explained. This should include a description of the internal and external context and any recent changes that affect the likelihood and impact of risks in general.

The scope of the risk assessment must also be defined. This may be expressed in terms of factors such as:

 Geographical location e.g. countries, offices, data centers  Organizational units e.g. specific departments

 Business process(es)

 IT services, systems and networks  Customers, products or services

## Identification of Risks

The process of identifying risks to be assessed will consist of the following steps in line with the requirements of ISO/IEC 27001. Risks are identified to the confidentiality, integrity or availability of information within the scope of the ISMS.

## Identify potential threats

Threats will be identified will vary according to the type of asset and could be accidental events such as fire, flood or vehicle impact or malicious attacks such as viruses, theft or sabotage. Threats will apply to one or more of the confidentiality, integrity and availability of the asset.

## Assess existing vulnerabilities

Attributes of an asset (or asset group) which may be exploited by any specific threat are referred to as vulnerabilities and will be detailed as part of the risk assessment.

## Identify risk scenarios

The identification of risks to the information security of the organization will be performed by a combination of group discussion and interview with interested parties.

Such interested parties will normally include (where possible):

 Head of departments responsible for each domain of business activity  Legal and Compliance team

 Any other party that is felt to provide useful input to the risk identification process

Identified risks will be recorded with as full a description as possible that allows the likelihood and impact of the risk to be assessed. Each risk must also be allocated an owner.

## Perform Risk Analysis

Risk analysis shall assign a numerical value to the 1 likelihood and 2 impact of a risk.

*Likelihood \* Impact  Total Risk*

Total risk shall be classified as level of high, medium or low. The Risk analysis process shall be recorded to aid understanding and replicability.

## Likelihood Determination

Risk likelihood is defined as the chance of a risk occurring to the organization. Risk likelihood will be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table 1.

When assessing the likelihood of a risk, existing controls will be considered. This may require an assessment to be made as to the effectiveness of existing controls.

|  |  |  |
| --- | --- | --- |
| **GRADE** | **DESCRIPTION** | **SUMMARY** |

|  |  |  |
| --- | --- | --- |
| 1 | Improbable | Has never happened before and there is no reason to think it is any more likely now |
| 2 | Unlikely | There is a possibility that it could happen, but it probably won't |
| 3 | Likely | On balance, the risk is more likely to happen than not |
| 4 | Very Likely | It would be a surprise if the risk did not occur either based on past frequency or current circumstances |
| 5 | Almost certain | Either already happens regularly or there is some reason to believe it is virtually imminent |

## Impact Determination

An estimate of the impact that the loss of confidentiality, integrity or availability could have on the organization must be given. This should consider existing controls that lessen the impact, as long as these controls are seen to be effective.

Consideration will be given to the impact in the following areas:

 Customers  Finance

 Health and Safety  Reputation

 Data

 Legal, contractual or organizational obligations

The impact of each risk will be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table 2.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **GRADE** | **DESCRIPTION** | **CUSTOMER IMPACT** | **FINANCIAL IMPACT** | **HEALTH & SAFETY** | **IMPACT ON REPUTATION** | **LEGAL IMPACT** |
| 1 | Negligible | No effect | Very little or none | Very small additional risk | Negligible | No implications |
| 2 | Slight | Some local disturbance to normal business operations | Some | Within acceptable limits | Slight | Small risk of not meeting compliance |
| 3 | Moderate | Can still deliver product/service with some difficulty | Unwelcome but could be borne | Elevated risk requiring immediate attention | Moderate | In definite danger of operating illegally |
| 4 | High | Business is crippled in key areas | Severe effect on income and/or profit | Significant danger to life | High | Operating illegally in some areas |
| 5 | Very High | Out of business; no service to customers | Crippling; the organization will go out of business | Real or strong potential loss of life | Very High | Severe fines and possible imprisonment of staff |

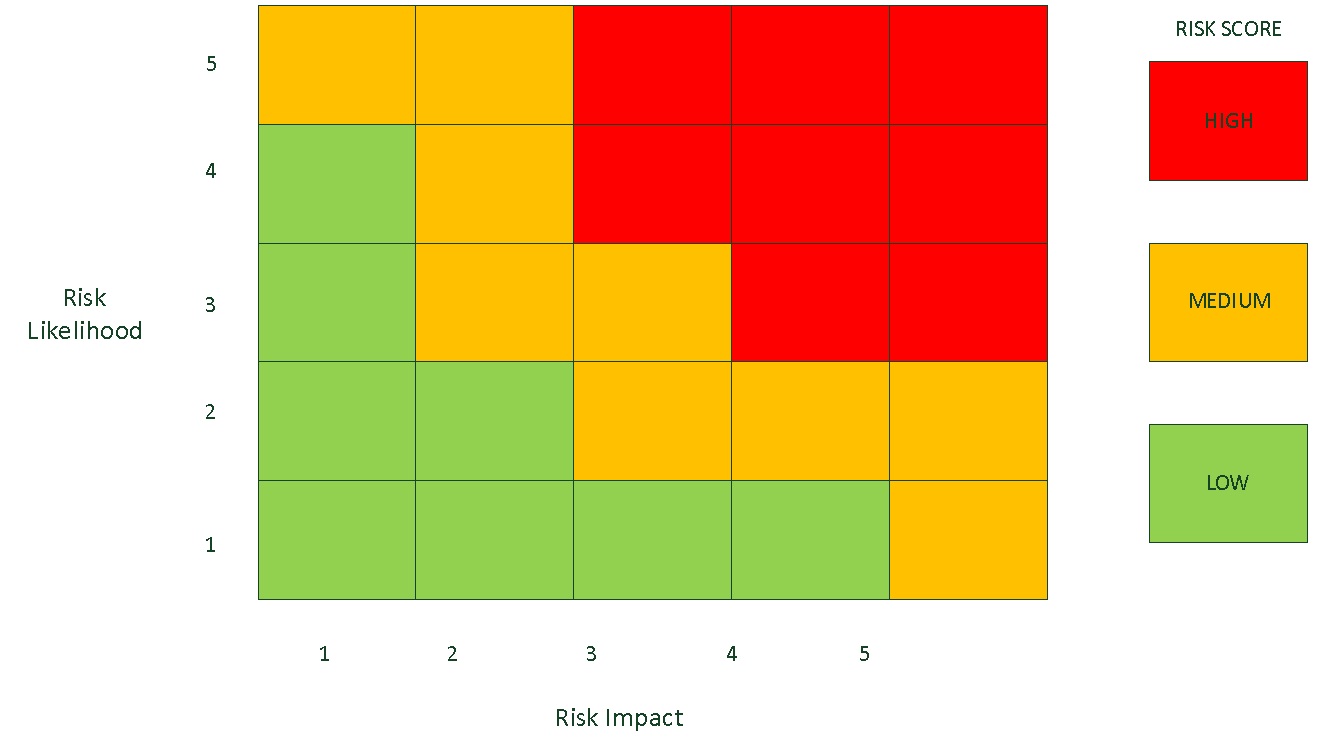
# Risk classification

Based on the assessment of the grade of likelihood and impact, a score is calculated for each risk by multiplying the two numbers. This resulting score is then used to decide the classification of the risk based on the matrix shown in figure 2.

Each risk will be allocated a classification based on its score as follows:  High: 12 or more

 Medium: 5 to 10 inclusive

 Low: 1 to 4 inclusive



*Figure 2 Risk matrix chart*

The classification of each risk will be recorded as input to the risk evaluation stage of the process.

## Risk evaluation

The purpose of risk evaluation is to decide which risks can be accepted and which ones need to be treated. Risks shall be considered on a case-by-base basis but will be defaultly evaluated as such:

|  |  |
| --- | --- |
| **Color** | **Action** |
| Green | The risk is low and typically able to be accepted. |
| Orange | Treatment is evaluated but risks in this tier may be accepted if compensating controls are in place. |
| Red | The risk is high and mitigation plans shall be drafted. |

Risks will be prioritized for treatment according to their score and classification so that very high scoring risks are recommended to be addressed before those with lower levels of exposure for the organization.

## Risk assessment report

A risk assessment report shall be prepared including the following:

 Likelihood  Impact

 Risk Score

 Risk Classification  Risk Owner

 Whether the risk is recommended for acceptance or treatment  Priority of risks for treatment

 Controls in place to mitigate risk

This report is input to the risk treatment stage of the process and must be signed off by management before continuing, particularly in respect of those risks that are recommended for acceptance.

# Risk treatment

The overall intention of risk treatment is to reduce the classification of a risk to an acceptable level. The following options may be applied to the treatment of the risks that have been agreed to **be unacceptable:**

 **Accept** the risk  Accepting risk, or risk acceptance, occurs when a business or individual acknowledges that the potential loss from a risk is not great enough to warrant spending money to avoid it.

 **Mitigate** the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk

 **Avoid** the risk by taking action that means it no longer applies

 **Share** the risk with another party e.g., insurer or supplier

Judgement will be used in the decision as to which course of action to follow, based on a sound knowledge of the circumstances surrounding the risk e.g.

 Business strategy

 Regulatory and legislative considerations  Technical issues

 Commercial and contractual issues

The GRC team will ensure that all parties who have an interest or bearing on the treatment of the risk are consulted, including the risk owner.

## Selection of controls for risk mitigation

In accordance with [Company Name]ʼs adoption of the ISO/IEC 27001 standard, Annex A of that document will be used as the starting point for the identification of appropriate controls to address the risk treatment requirements identified as part of the risk assessment exercise.

The controls set out in Annex A will be supplemented by the extended and additional guidance set out in the following codes of practice:

 ISO/IEC 27002  Code of practice for information security controls

 ISO/IEC 27018  Code of practice for protection of personally identifiable information PII in public clouds acting as PII processors

## Statement of applicability

The Statement of Applicability will set out those controls from Annex A of the ISO/IEC 27001 standard that have been selected and the reasons for their selection. It will also detail those that have been implemented and identify any that have been explicitly excluded together with a reason for such exclusion.

# Management approval

At each stage of the risk assessment process management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. Management will approve the following documents:

 Risk Assessment Report  Risk Treatment Plan

 Statement of Applicability

Signoff will be indicated according to [Company Name] documentation standards. In addition to overall management approval, the acceptance or treatment of each risk must be signed off by the relevant risk owner.

# Risk monitoring and reporting

As part of the implementation of new controls and the maintenance of existing ones, risk will be monitored continuously by the GRC team. The annual risk assessment results shall be communicated to top management.

# Regular review

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid.

# Maintenance of the Risk Register/Treatment Plan

A Risk Register/Treatment Plan shall be documented on [Company Name]ʼs internal wiki. The risk treatment plan and risk register will detail:

 Risks requiring treatment  Risk owner

 Recommended treatment option  Control(s) to be implemented

 Responsibility for the identified actions

 Cost estimate for implementing the control(s)  Timescales for actions

 Expected residual risk levels after the controls have been implemented

This plan will be reviewed by GRC and the relevant risk owner(s) to show agreement to the actions identified and to the levels of residual risk remaining after the treatment actions have been completed.

For each risk identified in the risk assessment report as needing to be treated, an approach has been agreed to take one or more of the following treatment options to reduce its risk level:

 **Mitigate** – take action to reduce either the likelihood or impact of the risk (or both)

 **Share** – agree or contract with a third party to share the effect of the risk

 **Avoid** – change the way we work or some other factor so that the risk no longer applies

The specific actions to be taken are then identified together with an action owner and a target timescale.

**Areas of the standard addressed**

The following areas of the ISO/IEC 270012013 standard is addressed by this document:  6 Planning

* 1. Actions to address risks and opportunities
     1. General
     2. Information security risk assessment
     3. Information security risk treatment  8 Operation

8.2 Information security risk assessment

8.3 Information security risk treatment Revision history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** | **Approved by** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |