Cyber Security Risk Management Plan

Table of Contents

[Background 3](#_Toc17190286)

[Purpose 3](#_Toc17190287)

[Definitions 3](#_Toc17190288)

[Acceptable Use Policy 4](#_Toc17190289)

[Physical Security 4](#_Toc17190290)

[Cyber Security 5](#_Toc17190291)

[Information Security 5](#_Toc17190292)

[Mobile Security 5](#_Toc17190293)

[Responsibilities 6](#_Toc17190294)

[Non-Compliance With This Policy 6](#_Toc17190295)

[Appendix A 7](#_Toc17190296)

[Appendix B 7](#_Toc17190297)

[IT Acceptable Use Assessment 11](#_Toc17190298)

# Background

**[Describe The Background Of Why A Cyber Security Risk Management Plan Has Come About.]**

The **[Business Name]** acknowledges the need to assess the security risks to the **[Business Name]** and permit treatment (mitigation) or acceptance of each identified risk to **[Business Name]**

Therefore, the **[Business Name]** is establishing Cyber Security Risk Management Framework to support the **[Business Name]** and assess identified risks which could negatively impact the **[Business Name]**

# Purpose

**[Describe What The Intent Of This Document Will Be.]**

This document sets forth the process to adequately assess identified risks to **[Business Name].** It establishes the business rules and guidelines for consistency and compliance in demonstrating the risk management approach used for **[Business Name]**

# Definitions

**[Define Any Terms That Are Used Throughout This Document.]**

|  |  |
| --- | --- |
| Terms | Definition |
| IT Asset | **IT Asset** refers to anything (tangible or intangible) that has value to an organisation, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualised computing), and related hardware (e.g., locks, cabinets, keyboards), as well as people and intellectual property (including software). |
|  |  |

# Overview

Today organisations cannot afford an ad-hoc approach to security. Instead, they need to identify, analyse and prioritise the risks to the confidentiality, integrity or availability of their data or information systems, based on both the likelihood of the event and the level of impact it would have on the business.

Risk assessments are primarily a business concept focused on ensuring the ability to maintain operation. The includes how the business makes money, how employees and assets affect the profitability of the business, and what risks could result in large monetary losses for the business.

Within the Cyber Security space, risk assessments primarily focus on identified security risk which could maintain or enhance business operations or which lead could lead to the largest financial losses to the business.

A basic risk assessment involves three main components. (1) The importance of the assets at risk, (2) How big the threat is, and (3) how vulnerable is the business to the threat. Using these three components will allow a business to assess the risk of impact or loss to the business.

# Risk Assessment Process

**[Describe The Details Of The Risk Assessment Process.]**

During a risk assessment it is essential to establish the business and technical context of the information system being reviewed. Establishing the context ensures that the businesses objectives are captured and that the internal and external factors that influence the risks are considered. It also sets the scope for the rest of the process.

**Business Context**

The following table is required to be completed to establish Business Context.

|  |  |  |
| --- | --- | --- |
| Title | Description | Response |
| Information Classification | What type of information is stored, processes and/or transmitted? |  |
| Business Process Supported | What business process and objectives are contributing to the business? |  |
| Users of The System | Who are the users of the system (internal, external)? What level of privilege do the users require? |  |
| Compliance Requirements | Are there any legal or regulatory requirements that are required to be adhered to? |  |
| Business Priority | What is the business priority? |  |

**Technical Context**

The following table is required to be completed to establish Technical Context.

|  |  |  |
| --- | --- | --- |
| Title | Description | Response |
| Business Owner | Who is the business owner who will be responsible the system? |  |
| Architecture | How does this integrate with existing systems? |  |
| Support | Who will be responsible for the ongoing support of the system? |  |
| Dependencies | What are the systems dependancies? |  |

## Risk Identification

The next phase of the risk assessment is to identify critical assets that the business is dependent on. This can be achieved by:

* Interview with management
* An analysis of existing systems
* Existing documentation
* Existing critical assets
  + Servers
  + Databases
  + Documents
  + Applications
  + Intellectual Property
  + Customer Private Information

## Risk Threat

The next phase of the risk assessment is to assess the potential threats. This can be determined by:

* Identifying Legal or Compliance Requirements
* System Breach
* Natural Disasters
* Accidental Data Loss
* Malicious Data Loss
* System Configuration
* System Failure

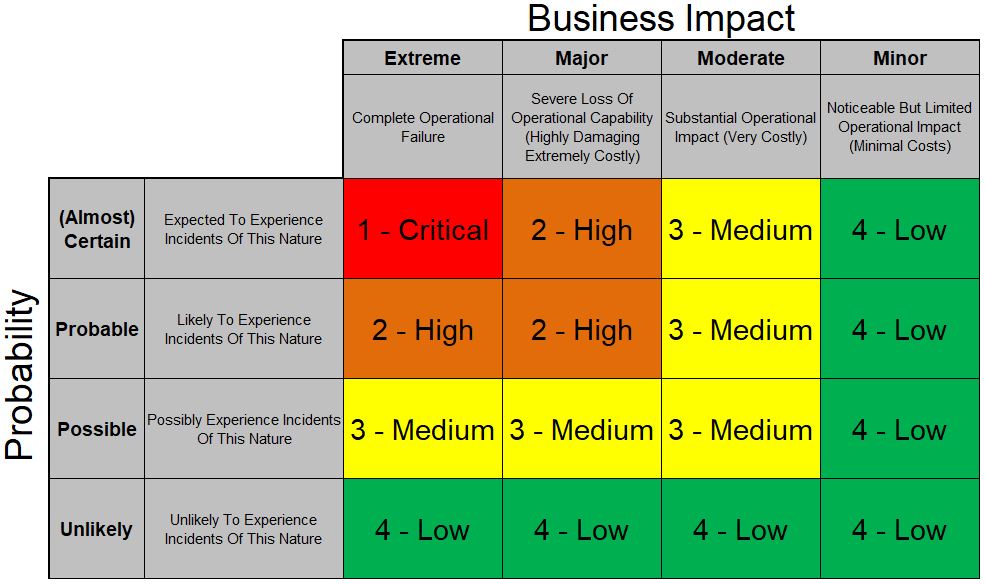
## Risk Consequence

The next phase of the risk assessment is to use the information gathered from the previous steps and determine the likelihood and consequence of the identified threats to the business. This can be achieved by:

* Interview with management
* Replacement Cost Analysis
* Qualitative Analysis
* Quantitative Analysis

## Risk Rating

The next phase of the risk assessment is to determine the Risk Rating. This can be achieved by using a Risk Matrix to determine the existing risk to the business.



Using the information gathered above will provide a clear picture of the probability of a threat being materialised and the impact it will have on the business.

## Existing Controls

The next phase of the risk assessment is to use the information gathered from the previous steps and assess the existing controls which are in place.

Existing controls can will reduce the overall risk and in some cases lower the risk rating to an acceptable level.

## Mitigating Controls

For identified risks which exceed the businesses risk tolerance, mitigating controls should be considered to implement and reduce the controls to an acceptable level.

## Risk Acceptance

Once the mitigating controls have been considered, the Risk Rating should be reviewed, and the business should determine if the risk should be accepted or transferred.

