**Information Security**

**Risk Assessment and Treatment**

**Process**

**Security Classification: Restricted**

**Document Ref. ISMS06002**

**Version: 1.0**

**Draft 1**

**Document Author: Cybersecurity Unit**

**Document Owner: TMP/NCS**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Change Number** | **Summary of Changes** |
| 1.1 |  | Draft 1 | Tailoring |
| 1.2 |  | Draft 1 | IE Review |
| 1.3 |  | Draft 1 | Legal Review |
| 1.4 |  |  | Sign-off |

**Document Review**

|  |
| --- |
| **Date of Next Scheduled Review** |
|  |

Distribution

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

**Contents**

[1 Introduction 5](#_Toc377990846)

[2 Risk Assessment and Treatment Process 6](#_Toc377990847)

[2.1 Criteria for Performing Information Security Risk Assessments 6](#_Toc377990848)

[2.2 Process Diagram 7](#_Toc377990849)

[2.3 Identification of Risks 8](#_Toc377990850)

[2.3.1 Assets 8](#_Toc377990851)

[2.3.2 Threats 8](#_Toc377990852)

[2.3.3 Vulnerabilities 8](#_Toc377990853)

[2.3.4 Likelihood 8](#_Toc377990854)

[2.3.5 Impacts 8](#_Toc377990855)

[2.4 Risk Analysis and Evaluation 9](#_Toc377990856)

[2.4.1 Numerical Classification 9](#_Toc377990857)

[2.4.2 Risk Acceptance Criteria 10](#_Toc377990858)

[2.4.3 Risk Assessment Report 10](#_Toc377990859)

[2.5 Risk Treatment 11](#_Toc377990860)Act

[2.5.1 Risk Treatment Options 11](#_Toc377990861)

[2.5.2 Risk Treatment Plan 11](#_Toc377990862)

[2.6 Selection of Controls 12](#_Toc377990863)

[2.6.1 Statement of Applicability 12](#_Toc377990864)

[2.7 Management Approval 12](#_Toc377990865)

[2.8 Risk Monitoring and Reporting 12](#_Toc377990866)

[2.9 Regular Review 13](#_Toc377990867)

[2.10 Roles and Responsibilities 13](#_Toc377990868)

[2.10.1 RACI Chart 13](#_Toc377990869)

[3 Conclusion 14](#_Toc377990870)

[4 Appendix A – List of Typical Threats 15](#_Toc377990871)

# Definition of terms

Risk assessment is a systematic process of identifying, analysing, and evaluating potential risks that could affect an organization's objectives, assets, operations, or projects. It involves identifying threats and vulnerabilities, assessing the likelihood and potential impact of adverse events, and prioritizing risks based on their significance. The goal of risk assessment is to provide decision-makers with valuable insights into the organization's risk profile, enabling them to make informed decisions about risk mitigation strategies and resource allocation.

## Introduction

The effective management of information security has always been a priority for the Project Management Office (PMO) to manage risk and safeguard its reputation.

However, there is still much to be gained by the PMO in introducing industry-standard best practice processes, not the least of which is the ability to become more proactive in our approach to information security and to gain and maintain a better understanding of our stakeholders needs and plans.

The PMO has started on the road to adoption of ISO/IEC 27001 and has completed staff training to foundation qualification level. As part of this process, it has decided to pursue full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an external third party.

# Risk Assessment and Treatment Process

Risk is the happening of an unwanted event, or the non-happening of a wanted event, which affects a business in an adverse way. Risk is realised when:

* the objectives of the business are not achieved.
* the assets of the business are not safeguarded from loss.
* there is non-compliance with organisation policies and procedures or external legislation and regulation.
* the resources of the business are not utilised in an efficient and effective manner.
* the confidentiality, integrity and availability of information is not reliable.

It is important that the PMO has an effective risk assessment and treatment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them.

It is important also that the process is sufficiently clear so that successive assessments produce consistent, valid, and comparable results, even when carried out by different people.

## Criteria for Performing Information Security Risk Assessments

There are several circumstances in which an information security risk assessment should be carried out and these will vary in scope. In general, these are as follows:

* A comprehensive risk assessment covering all information assets as part of the initial implementation of the Information Security Management System (ISMS)
* Updates to the general risk assessment as part of the management review process – this should identify changes to assets, threats, and vulnerabilities and therefore risk levels.
* As part of projects that involve significant change to the Organisation, the ISMS, or its information assets.
* As part of the change management process when assessing whether proposed changes should be approved
* On major external change affecting the organisation which may invalidate the conclusions from previous risk assessments e.g., changes to relevant legislation.

If there is uncertainty regarding whether a risk assessment is appropriate, the Organisation should err on the side of caution and carry one out.

## Process Diagram

The process of risk assessment and treatment is shown in the diagram below.



*Fig 1 – Risk Assessment and Treatment Process*

Each step in this process is described in more detail in the rest of this document.

## Identification of Risks

The process of identifying risks will consist of the following steps in line with the requirements of ISO/IEC 27001.

### Assets

A full inventory of assets will be compiled and maintained at the PMO. The definition of an asset is taken to be “anything that has value to the organisation” and is therefore worthy of protection. This will include physical assets such as IT servers and operational machinery as well as information assets such as client lists and application databases.

The list of assets is held in document [ISMS14001 Information Asset Inventory](../A8.%20Asset%20management/ISMS14001%20Information%20Asset%20Inventory.xls) as part of the ISMS.

### Threats

For each asset, the threats that could be reasonably expected to apply to it will be identified. These 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. An initial starting list of typical threats is at [Appendix A](#_Appendix_A_–) of this document.

### Vulnerabilities

Circumstances or attributes of an asset which may be capitalised on by any specific threat will be detailed. Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of malware) or the existence of paper files in a data centre (which could be exploited by the threat of fire).

### Likelihood

An estimate of the likelihood of the threat occurring must be made. This should consider whether it has happened before either to the Organisation or similar organisations in the same industry or location and whether there exists sufficient motive, opportunity, and capability for the threat to become real.

### Impacts

Finally, an estimate of the impact that the loss of confidentiality, integrity or availability of the asset could have on the Organisation should be given.

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

* Clients
* Finance
* Health and Safety
* Reputation
* Knock-on impact within the Organisation
* Legal, contractual, or organisational obligations

## Risk Analysis and Evaluation

### Numerical Classification

To assess the risk to an asset and determine the appropriate treatment, the Project Management Office will examine the threats, vulnerabilities, the likelihood that the threat will take place and the impact of it should it occur. A 5-point scale will be used to describe the likelihood of a risk-taking place and also to describe the impact that it is likely to have.

The 5-point scale for the likelihood ranges from 1=improbable to 5= certain; the 4-point scale for the impact ranges from 1=negligible to 5=very high. The risk matrix shown below illustrates the scales and allows us to prioritise our risks so that they can be managed more effectively.

**5** certain

**4** Almost Certain

**3** Very Likely

**2** Unlikely

**1** improbable

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | HIGH |  |
| LIKELIHOOD |  |  |  |  |
|  | MEDIUM |  |  |  |
| LOW |  |  |  |  |
|  |  |  |  |  |

2

Low

1

Negligible

4 High

3 medium

5

IMPACT

*Fig 2 - Risk Matrix Chart*

The risk classification used will be the score obtained from multiplying the likelihood that the risk will occur and the impact it is likely to have. Both scales range from 1 to 5, so the minimum score will be 1 and the maximum score will be 5 as shown in the matrix above.

Each risk will be allocated a classification based on its score as follows:

* HIGH 16-25
* MEDIUM 6-15 inclusive
* LOW 1 to 5 inclusive

The rationale for indicating the likelihood and impact ratings awarded will be given so that these can be assessed later to see if they have materially changed. This will also assist in ensuring consistency and repeatability in risk assessments.

### Risk Acceptance Criteria

The matrix in *Figure 2* shows the classifications of risk, where green indicates an acceptable threshold as the likelihood is minimal or/and the impact is minimal. The yellow indicates that the risk threshold is medium as the risk is larger as is the impact; so, containing those risks is more important than addressing those in the green. The red area indicates the risks that are of the highest priority as both the impact and the risk are relatively high, so measures to contain them must be of the highest priority and, if they cannot be reduced then countermeasures must be in place for these risks.

The overall intention of the risk assessment and proposed treatments is to reduce the classification of the risks to an acceptable level e.g., HIGH down to MEDIUM or MEDIUM down to LOW. This is not always possible as sometimes although the score is reduced, it remains in the same classification e.g., reducing the score from 8 to 6 means it remains a MEDIUM level risk. The organisation may decide to accept these risks even though they remain at a MEDIUM rating.

The priorities of the items in the Continual Improvement Plan are determined by the highest priority of the Risk Assessment items addressed e.g., if 3 items are addressed by a single action and one is MEDIUM and two LOW, then the priority of the action will be MEDIUM.

### Risk Assessment Report

The output from the Risk Analysis and Evaluation stage is the Risk Assessment Report. This shows the following information:

* Assets
* Threats
* Vulnerabilities
* Controls currently implemented.
* Likelihood (including rationale)
* Impact (including rationale)
* Risk Score
* Classification
* Risk Owner
* Whether the risk is accepted or needs treatment

This report is input to the Risk Treatment stage of the process and must be signed off by management before continuing.

## Risk Treatment

For those risks that are judged to be above the threshold for acceptance by the PMO management, the options for treatment will then be explored.

### Risk Treatment Options

The following options may be applied to the treatment of the identified unacceptable risks:

1. Apply appropriate controls to lessen the likelihood and/or impact of the risk.
2. Avoid the risk by taking action that means it no longer applies.
3. Transfer the risk to another party e.g., insurer.

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.

* Operational strategy
* Regulatory and legislative considerations
* Technical issues
* Commercial and contractual issues

The Risk Manager will ensure that all parties who have an interest or bearing on the treatment of the risk are consulted.

### Risk Treatment Plan

The evaluation of the treatment options will result in the production of the Risk Treatment Plan which will detail:

* Risks above the acceptance threshold.
* Assets affected.
* Recommended treatment option.
* Control Requirements.
* Cost implications.

This document will be input to the next stage in the process where controls will be selected to meet the identified requirements.

## Selection of Controls

In accordance with the PMO adoption of the ISO/IEC 27001 standard, Annex A of this 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.

If the controls set out in Annex A do not address all requirements, then additional controls may be implemented.

## Statement of Applicability

The [ISMS06005 Statement of Applicability](ISMS06005%20Statement%20of%20Applicability.xls) 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 PMO documentation standards.

In addition to overall management approval, each treatment should 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, key performance indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be reported on a regular basis and trend information produced so that exception situations can be identified and dealt with by 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. The relevant risk assessments will also be reviewed upon major changes to the Organisation such as office moves, expansions or introduction of new IT Organisations.

## Roles and Responsibilities

Within the process of risk assessment there are several key roles that play a part in ensuring that all risks are identified, addressed and managed. These roles are shown in the Responsible, Accountable, Consulted, and Informed (**RACI**) table below, together with their relative responsibilities at each stage of the process.

## RACI Chart

The table below clarifies the responsibilities at each step using the RACI model, i.e.:

R= Responsible A= Accountable C= Consulted I= Informed

| **Role:** | **Cybersecurity Unit** | **Risk Management Unit** | **Operational personnel** |
| --- | --- | --- | --- |
| **Step** |
| Identify the risks | A/R | C | C |
| Risk Acceptance Criteria | C | A/R | C |
| Analyse and evaluate the risks | A/R | C | C |
| Identify and Evaluate Options for Treatment | A/R | C | C |
| Select Control Objectives and Controls | A/R | C | C |
| Obtain Management Approval for Residual Risks | A | R | C |
| Monitor and Report | A/R | I | C |
| Regular Review | A/R | C | C |

Further roles and responsibilities may be added to the above table as the Risk Assessment and Treatment Process matures within the Nigeria Customs Organisation.

# Conclusion

The process of risk assessment and treatment is fundamental to the implementation of a successful Information Security Management System (ISMS) and forms a significant part of the ISO/IEC 27001 standard.

By following this process, the Project Management Office will go some way to ensuring that the risks that it faces in the day-to-day operations are effectively managed and controlled.

# Appendix A – List of Typical Threats

The following list may be used as a starting point for creating a relevant list of threats which may apply to the information assets identified in the inventory.

| **Threat Category** | **Threat** | **Example** |
| --- | --- | --- |
| Human | Malicious outsider | Someone launches a denial-of-Organisation attack on the Project Management Office system. |
|  | Malicious insider | An officer or trusted third party accesses information in an unauthorised manner from inside the Organisation network |
|  | Loss of key personnel | One or more people with key skills or knowledge are unavailable perhaps due to extended sickness |
|  | Human error | An officer accidentally deletes the client database |
|  | Accidental loss | Personnel loses a device containing restricted document(s). |
|  |  |  |
| Natural | Fire | The office(s) burns down due to an electrical fault |
|  | Flood | The nearby river breaks its banks, and an office is severely flooded |
|  | Severe weather | No-one can get into the office due to the weather |
|  | Earthquake | The area of an office is affected by an earth tremor that damages servers |
|  | Lightning | All servers are fried by a lightning strike on the data centre building |
|  |  |  |
| Technical | Hardware failure | A key server has a processor failure |
|  | Software failure | A system processes SGD/PAAR(s) incorrectly due to a bug |
|  | Virus/Malicious code | A virus spreads throughout the network preventing access to data |
|  |  |  |
| Physical | Sabotage | A disgruntled ex-officer takes an axe to the server room |
|  | Theft | You come in on Monday morning to find all of the PCs have been stolen |
|  | Arson | Someone with a grudge against the Organisation starts a fire during the night |
|  |  |  |
| Environmental | Hazardous waste | A lorry carrying hazardous waste has an accident outside the office |
|  | Power failure | The sub-station supplying the area has a meltdown |
|  | Gas supply failure | There is a suspected leak, and all supplies are turned off |
|  |  |  |
| Operational | Process error | The new data transfer procedure doesn't cater for unexpected circumstances and data is lost or sent to the wrong destination |
|  | Crime scene | A crime happens in or near the office and the area is sealed off by police |