AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

The purpose of this procedure is to establish a system on how information security risk assessments will be carried out and the resulting risks treated.

SCOPE

This procedure will take place at several levels within the Information Security Management System (ISMS) and is qualitative in nature in that it uses the terms high, medium, and low to describe the relative classification level for each specific risk.

REFERENCE

ISO/IEC 27001 Standard	6.1.2 / 8.2 Information security risk assessment 6.1.3 / 8.3 Information security risk treatment

DEFINITIONS

Risk	Effect of uncertainty on objectives
Risk Acceptance	Informed decision to take a particular risk
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk Owner	Person or entity with the accountability and authority to manage a risk
Risk Treatment	Process to modify risk

RESPONSIBILITIES & AUTHORITIES

The Top Management has the prime responsibility and approval authority for this procedure.

Process owners shall take the role of risk owners and shall participate in carrying out the risk assessment and risk treatment for their functions / processes.

The ISMS Management Representative (MR) is responsible to guide the process owners and shall review, collate and compile the risk assessment results and treatment plans for effective monitoring.

PROCEDURE

A. Criteria for Performing Risk Assessment

There are a number of criteria that determine when an information security risk assessment should be carried out and these will vary in scope.

In general, a risk assessment should be performed in the following circumstances:

- A comprehensive risk assessment to identify risks associated with the loss of confidentiality, integrity, availability, and/or privacy of information within the scope of the established ISMS
- Updates to the comprehensive risk assessment as part of the regular review (annually) intended to identify changes to risk scenarios and possibly risk levels
- When selecting new suppliers or any change in suppliers or the contracts with them
- On major external change affecting the organisation which may invalidate the conclusions from previous risk assessments e.g., changes to relevant legislation, mergers and acquisitions, new ICT systems
- As part of software development or during the design of the solution and before they are commissioned

If there is uncertainty regarding whether it is appropriate to carry out a risk assessment, the process owner should err on the side of caution and ensure that one is performed.

B. Risk Assessment

1. Establish the Context

The overall environment in which the risk assessment is carried out should be considered. This includes internal issues, external issues, interested parties and any recent changes that affect the likelihood and impact of risks in general.

2. Risk Identification

For the purpose of risk assessment, it is important to understand the threats that could possibly apply to the organisation's information assets and the attributes of the information assets which may be exploited by any specific threat which are referred to as the asset vulnerabilities. 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 tangible information assets (which could be exploited by the threat of fire). Threats will vary according to the type of asset and could be accidental events such as fire and human error, or malicious attacks such as viruses, theft or sabotage. After understanding the threats and vulnerabilities, threat events (scenarios) and risks to the confidentiality, integrity, availability and/or privacy of information now be identified.

3. Risk Analysis

Risk analysis involves assigning numerical value to the: a) likelihood and b) impact of a risk. These values are then multiplied to arrive at a classification level of high, medium or low for the risk.

An estimate of the likelihood of a risk occurring must be made. When assessing the likelihood of a risk, existing controls should be taken into account. This may require an assessment to be made as to the effectiveness of existing controls.

Score	Likelihood	Description	Indicative Probability (of occurrence in a year)
1	Rare	The event may occur only in exceptional cases.	<5%
2	Unlikely	The event could occur at some time.	≥5% - 20%
3	Possible	The event should occur at some time.	≥21% - 40%
4	Likely	The event shall probably occur in most circumstances.	≥41% - 60%
5	Highly Likely	The event will occur in most circumstances.	≥61%

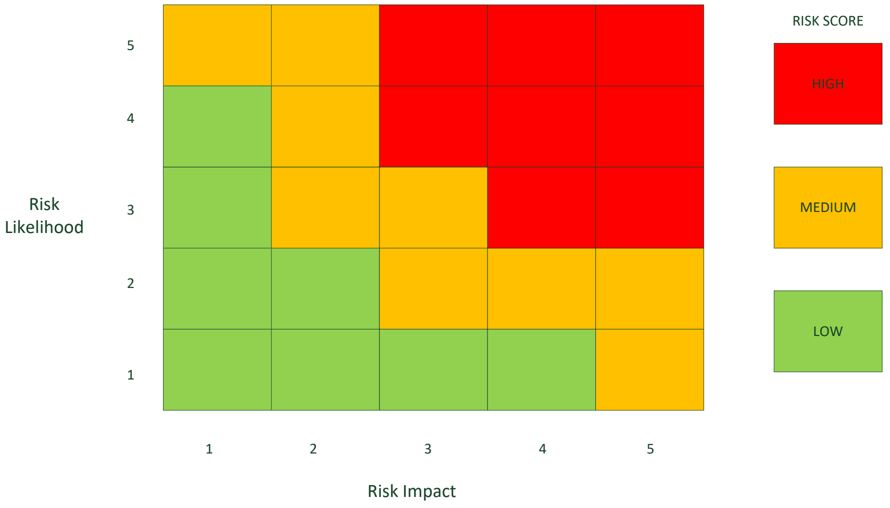
Similarly, an estimate of the impact of the threat events (scenario) and risks to the information must be made. Consideration should be given to the impact in the following areas: a) technological (data breach and system downtime); b) business (financial and operational); c) environmental, social and governance (environmental, reputational, legal/compliance).

Score	Impact	Technological		Business		Environmental, Social and Governance (ESG)		
		Data	**System Downtime**	**Financial Impact**	**Operational**	**Environmental**	**Reputational**	**Legal /Compliance**
1	Trivial	Leakage of confidential information to unauthorised internal parties (those that should not have user access to the materials)	Some parts of the system not visible to some users	$10K and below	Loss of a few small clients	Minimal and local impact which can be resolved	Tarnishing of company's image in public due to misconduct but no noticeable or measurable effect, no mention of incident in any media	Advisory / recommendation received from authorities
2	Minor	Leakage of confidential information to an unauthorised external party, but able to contain the leakage internally	Some parts of the system not visible to majority of users	Above $10K to $50K	Loss of several small clients	Limited local impact	Minor damage to brand image/ perception among small number of customers/ minor coverage of incident in local media	Warnings from authorities
3	Moderate	Leakage of confidential information to unauthorised external parties, but able to contain the leakage internally	System down for 4 hours or less	Above $50K to $100K	Loss of a few major clients	Widespread / short term impact	Adverse media reports in lesser-known regional media platforms – brand fails to meet customer needs in some areas, but customer preference remains largely unchained	Financial penalties below $100K
4	Major	Data privacy breach, but able to contain the breach internally without external help	System down for > 4 hours to 1 day	Above $100K to $200K	Loss of several major clients	Widespread / long term impact	Adverse media reports in local prominent media platforms – brand perception badly	Penalties above $100K to $200K

Score	Impact	Technological		Business		Environmental, Social and Governance (ESG)		
		Data	System Downtime	Financial Impact	Operational	Environmental	Reputational	Legal /Compliance
							damaged. Brand not 1st or 2nd choice	
5	Severe	Data privacy breach and need external help with containing the breach	System down for more than 1 day	$200K & above	Loss of all existing clients	Catastrophic	Reputation under severe threat – Widespread and irreversible perception that brand fails to meet most client's needs / significant coverage in national and international media	May lead to loss of license to operate business / penalties of $200K and above / imprisonment of board member(s)

4. Risk Evaluation

Based on the assessment of the grade of likelihood and impact, a resulting 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 below.



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

- High - 12 and above (red)
- Medium - 5 to 10 inclusive (orange)
- Low - 1 to 4 inclusive (green)

Risk will be prioritized for treatment according to their score so that the high scoring risks are recommended to be addressed with urgency before those with lower levels of exposure. The identified risks and the corresponding analysis and evaluation will be recorded in *ISMS-PR-01-F1 Risk Assessment & Risk Treatment Worksheet.*

C. Risk Treatment

1. Risk Appetite and Risk Strategies

In general terms, the organisation's appetite for risk may be said to be "Low" with the strategy to invest resources in mitigating risks to as low as reasonably practicable through effective security measures.

This general level of risk appetite will be applied to the risk assessments that are to be carried out as part of the ISMS and will determine the actions that need to be taken to mitigate the risk to an acceptable degree. The organisation's risk strategies can be summarized as follows:

Risk Score	Risk Strategies
Low (1-4)	Accept low risks and monitor them to ensure that the risk level assigned is accurate and does not increase over time.
Medium (5-10)	Treat the risks by ensuring measures are in place to mitigate them to as low as reasonably practicable within a defined time period.
High (12 and above)	Put measures in place to lower the risk to at least medium level within a prioritised time period for management attention.

2. Risk Acceptance Criteria

One of the treatment options is to ***accept the risk*** – knowingly and objectively accepting risks, provided that they clearly satisfy the organisation's policy and the criteria for risk acceptance; and in view of the cost effectiveness and business efficiency. This is a valid approach but must be used with caution.

A risk may be recommended for acceptance to the top management if it meets one or more of the following criteria:

- the risk of potential loss in confidentiality, integrity, availability and/or privacy of information calculated as 4 or less (low risk and is therefore within the organisation's risk appetite)
- the cost of an appropriate control is judged to be more than the potential loss
- known changes within 3 months or less will soon mean that the risk is reduced or disappears completely
- an area is known to be high risk but also high potential reward and the potential direct or indirect benefits are agreed to be greater than the impact i.e., it is a calculated risk (although, this acceptance criteria is not applicable in the context of personal data due to the consideration of risks to affected individuals)

Decisions to accept risks above the organisation's risk appetite (low) must be recorded with a suitable explanation and management sign-off.

3. Other Risk Treatment Options

For those risks that can't be accepted, the following options may be applied to the treatment of those risks:

- ***Mitigate*** the risk – applying appropriate controls to reduce the risk likelihood or risk impact or both
- ***Avoid*** the risk – removing and eliminating the risk by removing its origin in its entirety. This treatment is not often applied unless terminating the activity which results in the risk arising does not materially affect the organisation
- ***Transfer*** the risk – implementing a strategy that transfers the risk to another party or parties, such as outsourcing the management of a service, developing contracts with service providers or insuring against the risk. The third-party accepting the risk shall be aware of and agree to accept this obligation, reducing the impact component of risk faced by the organisation.

All parties who have an interest or bearing on the treatment of the risk should be consulted by the risk owner as and where applicable for the identification of appropriate controls to be implemented in the context of risks to information security.

Timescales and responsibilities for the identified actions must be recorded. Post-treatment analysis shall be conducted by the risk owner to check the effectiveness of the implemented actions to lower down the risk level. The risk owner shall sign off the acceptance of any residual risk after the post-treatment analysis or shall decide for additional controls to be implemented as necessary to further lower down the residual risks to an acceptable level based on the organisation's risk acceptance criteria. All these will be reflected in the *ISMS-PR-01-F1 Risk Assessment & Risk Treatment Worksheet.*

D. Statement of Applicability

The organization shall come up with the *ISMS-PR-01-F2 Statement of Applicability* (SOA) that will set out those controls from 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 according to the organization's information security context. Justification for such exclusion can include where the controls are not deemed necessary by the risk assessment, contractual requirements, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to personal data.

E. Risk Monitoring and Review

As part of the implementation of new controls and the maintenance of existing ones, progress will be reported during the regular information security meetings (at least once per quarter) so that exception situations can be identified and dealt with. Completion of actions listed in the treatment plans shall be monitored based on the timescale indicated.

The regular review of the risk assessments is intended to ensure that they remain current and the applied controls are valid. Relevant risk assessments will also be reviewed upon major changes to the business such as office moves, mergers and acquisitions, or introduction of new or changed processes and information and communication technology services which may have an impact to information security.

F. Risk Treatment and Communication

To ensure effective implementation of risk treatment, communications should be conducted before commencement of any new changes or introduction of new risk treatment, and at periodic intervals deemed appropriate but no longer than 1 year.

The risk owner who oversees the activities or areas where the risks exist shall ensure the person involve or may be involved in the activities exposed to the risks is informed of:

- The nature of the threats and vulnerabilities
- Any control or policy implemented
- Risk treatment to reduce the risks

Communication channels may include the following:

- Regular internal briefing sessions (interval should not be longer than 1 year)
- Emails

FORMS

ISMS-PR-01-F1	Risk Assessment and Treatment Worksheet
ISMS-PR-01-F2	Statement of Applicability