

CONTENTS

1	INTRODUCTION	2
1.1	Importance of Cybersecurity Risk Assessment	2
1.2	Common Problems Observed	2
2	PURPOSE, AUDIENCE & SCOPE	4
2.1	Purpose of Document	4
2.2	Audience & Scope	4
3	ESTABLISH RISK CONTEXT	5
3.1	Define Risk	5
3.2	Determine Risk Tolerance	6
3.3	Define Roles and Responsibilities	7
4	CONDUCT RISK ASSESSMENT	8
4.1	Step 1: Risk Identification	8
4.2	Step 2: Risk Analysis	11
4.3	Step 3: Risk Evaluation	16
5	RESPOND TO RISKS	18
5.1	Types of Risk Response Options	18
5.2	Choosing the Appropriate Risk Response Actions	19
6	REFERENCES	20
	ANNEX	21
	Summary of Expectations for CIIOs	21

1 INTRODUCTION

1.1 Importance of Cybersecurity Risk Assessment

With rapid advancement in technology, shifting cyber threat landscape and increased digitalisation, organisations may be exposing themselves to greater cybersecurity risks that may potentially have an adverse impact to their organisation and business objectives. Thus, it is imperative for organisations to manage these cybersecurity risks effectively.

Cybersecurity risk assessment (referred to as “risk assessment”) is an integral part of an organisation’s enterprise risk management process. By conducting a risk assessment, organisations would be able to:

- Identify “what could go wrong” events that are often a result of malicious acts by threat actors and could lead to undesired business consequences.
- Determine the levels of cybersecurity risk that they are exposed to. A good understanding of the risk levels would allow an organisation to dedicate adequate action and resources to treat risks of the highest priority.
- Create a risk-aware culture within the organisation. Risk assessment is an iterative process that involves engaging employees to think about technology risks and how they align to business objectives.

1.2 Common Problems Observed

While organisations recognise that risk assessment is an important part of their enterprise risk assessment practice, many struggled with the process to conduct a proper risk assessment. Some of the common gaps observed include the following:

- **Poor articulation of risk scenarios** – Risk scenarios describing “what could go wrong” events were often vague and generic without articulating specific threat events, vulnerabilities, assets and consequences. As a result, it is difficult to understand the extent of the risks, relate them to the organisational context, or identify targeted measures to address the risks.
- **Identification of risks using a compliance-oriented approach** – Many organisations identify risks from the point of assessing security controls (or lack thereof), similar to performing a compliance audit or gap analysis against a set of defined standards. A compliance-oriented approach towards risk assessment drives a “checklist” behaviour, giving a false sense of security that an organisation is not exposed to any risks as long as they fulfil all compliance requirements.

- **Absence of risk tolerance** – Organisations often do not integrate their cybersecurity risk management plans into their enterprise risk management programme. As a result, cybersecurity risk tolerance at the enterprise level is often ignored, and management face difficulty in deciding the appropriate level of risk-taking to adopt whilst in pursuit of their organisation’s business objectives.
- **Determining risk likelihood based on historical or expected occurrences** – Organisations have traditionally used the measure of time/frequency (e.g. historical or expected occurrences of events) to estimate their risk likelihood. The approach may be inaccurate when it is based on the number of times an incident has occurred previously, especially when there is lack of information on past cybersecurity incidents. In the context of cybersecurity, the likelihood of a cybersecurity incident is independent of the frequency of past occurrence.
- **Treating risks with irrelevant controls/measures** – Organisations may take a broad approach in coming up with measures to mitigate identified cybersecurity risks, resulting in the implementation of controls that do not fully address the root cause. This often stems from a poor understanding or articulation of risk scenarios.

2 PURPOSE, AUDIENCE & SCOPE

2.1 Purpose of Document

The purpose of this document is to provide guidance to Critical Information Infrastructure Owners (CIIOs) on how to perform a proper cybersecurity risk assessment.

This document will also identify expectations that are required of CIIOs to take note when performing their risk assessment. The expectations are denoted with the icon below in this guidance document.



2.2 Audience & Scope

This document is meant for use by both internal and external stakeholders but not limited to, the following:

- Stakeholders (e.g. business unit heads, system owners, Chief Information Security Officers, etc.) within any organisations, including CIIOs
- External consultants or service providers conducting risk assessment on behalf of organisations.

The scope of this guidance focuses only on the areas of risk framing, assessment and treatment. Other areas such as risk monitoring and reporting, which comes under a wider domain of risk management, is beyond the scope of this guidance.

3 ESTABLISH RISK CONTEXT

Establishing risk context is an important pre-requisite for conducting risk assessment. This step ensures that internal and external stakeholders involved in the risk assessment exercise have a common understanding of how the risk is framed, the risk tolerance to consider and the responsibilities of the risk owner.

3.1 Define Risk

There are many definitions of cybersecurity risk. Hence, before going further into the details of conducting a risk assessment, it is important to establish a common definition of cybersecurity risk. For the purpose of this guidance document, risk is defined as the function¹ of:

- The likelihood of a given threat event exercising on a vulnerability of an asset; and
- The resulting impact of the occurrence of the threat event

$$\text{Risk} = \text{Function} (\text{Likelihood}, \text{Impact})$$

Each of the risk factors mentioned in the definition is explained below.

Threat Event

Threat event refers to any event during which a threat actor², by means of threat vector³, acts against an asset in a manner that has the potential to cause harm. In the context of cybersecurity, threat events can be characterised by the tactics, techniques and procedures (TTP) employed by threat actors.

Vulnerability

Vulnerability refers to a weakness in the design, implementation and operation of an asset, or the internal control of a process.

Likelihood

Likelihood refers to the probability that a given threat event is capable of exploiting a given vulnerability (or set of vulnerabilities). The probability can be derived based on factors namely, discoverability, exploitability and reproducibility.

¹ The function of risk is adapted from National Institute of Standards and Technology Special Publication 800-30 Revision 1 (NIST SP 800-30R1)

² Threat actor refers to a person or entity that is responsible for an event that has the potential to cause harm.

³ Threat vector refers to the path or route that a threat actor uses to attack a target.

Impact

Impact refers to the magnitude of harm resulting from a threat event exploiting a vulnerability (or set of vulnerabilities). The magnitude of harm can be estimated from the perspective of a nation, organisation, or individual.

3.2 Determine Risk Tolerance

Risk tolerance⁴ is defined as the level of risk taking acceptable to achieve a specific business objective. Determining risk tolerance allows the Management to articulate how much risk the organisation is willing to accept.

A well-defined risk tolerance should articulate:

- Expectations for treating and pursuing specific types of risk
- Boundaries and thresholds of acceptable risk taking

Figure 1 below is an example of a risk tolerance table and must be tailored according to each organisation's context.

Risk Level	Risk Tolerance Description
Very High	This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately.
High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 month.
Medium High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months.
Medium	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately.
Low	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately.

Figure 1: An example of how risk tolerance is represented

⁴ Sources such as ISACA define *risk tolerance* as "the acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursue its objectives", and use the term *risk appetite* to refer to "the amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission". This guidance document does not distinguish between risk tolerance and risk appetite as we view them both to broadly mean the same (i.e. how much risk an organisation is willing to accept).

**CIIOs to note:**

In the CII risk assessment report, risk tolerance levels must be clearly defined.

3.3 Define Roles and Responsibilities

To ensure that stakeholders are aware of their expected roles in a risk assessment exercise, it is important to state them clearly upfront. Key roles in a risk assessment exercise include:

Head of Organisation

Highest-level senior official within the organisation with the overall responsibility and accountability for ensuring risks are appropriately managed within the organisation's tolerance level, and accepting all residual risks.

Business Owner

Highest-level senior official of a business unit responsible for ensuring that business activities meet business goals, or share concerns on the impact of system disruptions to the business.

Risk Management Function

An individual or group within the organisation responsible for the organisation-wide risk management approach. They should serve as a bridge between the technical and business function during risk assessment process, and provide oversight of the risk assessment activities to ensure consistent risk-based decisions.

Technology and Operations Function

An individual or group within the organisation that is responsible for the maintenance and operations of the technological infrastructure, including network and applications, to support the running of the system(s) supporting business activities. They should know the system assets and technical operations very well, and be able to advise on the technical impact for a compromised system.

Cybersecurity Function

An individual or group within the organisation responsible for the implementation and maintenance of cybersecurity controls in system(s) supporting business activities. They should identify the potential threats to a system, conceptualise cybersecurity risk scenarios, determine risk likelihood, as well as advise the appropriate measures to address the identified threats/attacks.

**CIIOs to note:**

In the CII risk assessment report, the stakeholders' roles and responsibilities in the risk assessment exercise must be clearly specified.

4 CONDUCT RISK ASSESSMENT

Risk assessment is about identifying risks that are specific to the environment, and determining the level of identified risks. The main steps in a risk assessment are risk identification, risk analysis and risk evaluation.



Figure 2: Process for Conducting Risk Assessment

4.1 Step 1: Risk Identification

Task A: Identify Assets

As the old security adage goes, “You can’t protect what you don’t know.” Therefore, the first task is to identify and create an inventory of all physical and logical assets that make up the system that is within the risk assessment scope. When identifying the assets, it is important to take note of those that are:

- **Crown jewels** - These assets are critical to achieving the overall business objectives and are usually what the attackers would actively seek to exploit

Example: In a Distributed Control System (DCS) of a power plant, a Programmable Logic Controller (PLC) controlling the turbine is likely to be considered a crown jewel as it directly affects the generation of electricity – the overall business objective of the power plant. An attacker who wants to disrupt power generation is likely to want to compromise and manipulate the logic within the PLC.

- **Stepping stones** - These assets are resources that attackers would want to take control and leverage to pivot across network segments before reaching the crown jewels.

Example: In a typical Windows environment, an Active Directory (AD) server that maintains/validate user login credentials to multiple servers is likely to be considered a stepping stone, as it provides a bridge for attackers to pivot into these servers.

Use the asset inventory list consolidated to create a network architecture diagram that provides a visual representation of the interconnectivity and communication paths between the assets. Identify and label all entry points (i.e. attack vectors) into the system, as well as the stepping stones and crown jewels. This would help facilitate the next task to identify threats.

Task B: Identify Threats

With the asset inventory list and network architecture diagram, identify the threat events that could exploit the vulnerabilities for each asset. There are many publicly available sources⁵ with threat libraries that can be referenced for identifying threat events.

Threats events can be systematically identified by taking the steps below:

- (i) Apply the threat events in the referenced libraries to each asset that presents an entry point⁶ (i.e. attack vector) to the system
- (ii) Document relevant threat events that are applicable to each asset
- (iii) Enumerate through the assets and repeat steps (i) and (ii) above until all key assets (especially crown jewels and stepping stones) are included

When enumerating through the assets to identify possible threat events, always keep in mind the attack stages of the Cyber Kill Chain⁷. The Cyber Kill Chain is a useful model that maps out steps and goals of a typical real-world attack. Threat events that are relevant to assets at the system perimeter are typically categorised in the early stages of the Cyber Kill Chain. As we move deeper into the system, threat events that are more relevant would be categorised in the later stages of the Cyber Kill Chain (e.g. lateral movement, command and control).

Task C: Construct Risk Scenarios

Constructing risk scenarios is the last task to complete the Risk Identification Step. This task aims to create “what could go wrong” scenarios that provide realistic and relatable view of risks based on the business context, system environment and pertinent threats.

A well-constructed risk scenario facilitates communication to stakeholders and allows for structured analysis of risks in subsequent steps. A risk scenario should articulate the following four (4) key elements:

- **Asset** - An object of value that has been identified in task A.

⁵ MITRE ATT&CK Knowledge Base and NIST SP800-30 (Annex E) are some examples of publicly available sources with useful threat libraries. The threat events within the libraries are categorised by tactics, techniques and procedures used by adversary.

⁶ Entry points could include front-end web application listening for HTTP requests, remote connection from vendor into application server via RDP, and open USB ports for removable media usage.

⁷ The Cyber Kill Chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack. The different stages of a Cyber Kill Chain are Reconnaissance, Weaponisation, Delivery, Exploit, Installation, Command and Control and Actions.

- **Threat event** - An attack event that has been identified in task B.
- **Vulnerability** - A weakness in the asset or processes supporting the asset that can be exploited by the identified threat event. The vulnerability may have surfaced in recent audits and/or penetration-tests, or may be relevant to the environment due to the use of certain technologies.
- **Consequence**⁸ - The direct result of the threat event.

Some examples of well-constructed risk scenarios are illustrated below.

Legend: Threat Event | Vulnerability | Asset | Consequence

Attacker performs an SQL injection on an **unpatched legacy web application** to **download sensitive patient medical records**.

Example 1: Risk Scenario

Internal staff makes a fraudulent payment instruction exceeding bank account balance on the **payment system** with **no set limit**, **resulting in a bank overdraft**.

Example 2: Risk Scenario

Unauthorised employee accesses the **SCADA server** using **default login credentials** and **execute shutdown command** to **disrupt the water supply to the entire east side of Singapore**.

Example 3: Risk Scenario

Attacker delivers spear-phishing email to **unsuspecting user**, which when clicked, triggers the **user account** to **perform SMB authentication with malicious server** and **discloses hashed credentials**.

Example 4: Risk Scenario



CIIOs to note:

In the CII risk assessment report, risk scenarios must include elements of threat event, vulnerability, asset and consequence.

⁸ The terms “consequence” and “impact” are often used interchangeably. However, they have different meanings and must not be confused. While “consequence” is the direct result of a threat event (e.g. power outage, disruption of services, loss of confidential data), “impact” is the degree to which consequence affects the business, operations etc (i.e. magnitude of harm).

4.2 Step 2: Risk Analysis

Risk analysis is about analysing the elements that make up each risk scenario to determine:

- The likelihood of a risk scenario occurring; and
- The impact (i.e. magnitude of harm) resulting from the occurrence of a risk scenario

Task A: Determine Likelihood

Historical or expected occurrence of an event has traditionally been used as a metric to measure the risk likelihood (e.g. Event is expected to occur once every year or has occurred once in the past year). However, the use of such a metric to measure cybersecurity risk likelihood may not be appropriate due to the dynamic nature of cybersecurity threats. A system that has not been compromised previously does not mean it would not be compromised in the future.

As a general guidance, the likelihood of cybersecurity risks should be assessed from the perspective of threats and vulnerabilities. One method to determine the cybersecurity risk likelihood is to consider the following factors⁹:

- **Discoverability** - How easy would an adversary be able to discover the vulnerability of an asset? This is dependent on the availability of information about the vulnerability and the exposure of the vulnerable asset.
- **Exploitability** - How easy would an adversary exploit the vulnerability of an asset? This is dependent on the access rights, complexity of tools, as well as technical skills required to carry out the attack.
- **Reproducibility** - How easy would an adversary be able to reproduce the attack on the asset? This is dependent on the complexity of the exploit customisation and the environmental conditions required to carry out the attack.

Figure 3 below is a sample assessment table to determine the cybersecurity risk likelihood based on the factors described above. The following steps can be taken to derive the likelihood score of a cybersecurity risk scenario:

- (i) Assign a score for each of the 3 likelihood factors (i.e. 1 – 5)
- (ii) Average the score and round off to the nearest whole number
- (iii) The final score will be the likelihood of the risk scenario; 5 being “Highly Likely” and 1 being “Rare”

⁹ The factors (Discoverability, Exploitability, and Reproducibility) are adapted from Microsoft’s DREAD model for threat assessment.

Likelihood Rating	Discoverability	Exploitability	Reproducibility
Highly Likely (5)	The vulnerability of the target: <ul style="list-style-type: none"> • can be discovered by searching / scanning the public domain for published information (e.g. Shodan, ExploitDB); • can be discovered and attacked from external networks (including the internet) 	The attack: <ul style="list-style-type: none"> • can be performed with no access rights of the target; • can be performed with publicly available tools without technical knowledge 	The attack: <ul style="list-style-type: none"> • can be repeated at will without any specific configuration¹⁰ or event condition¹¹ • can be repeated at will without any customisation of the published exploits
Likely (4)	The vulnerability of the target: <ul style="list-style-type: none"> • can be discovered by probing the target (e.g. port scans); • can be discovered and attacked from adjacent subnets or network segments 	The attack: <ul style="list-style-type: none"> • can be performed with restricted access rights of the target (e.g. user); • can be performed with publicly available tools with basic technical knowledge 	The attack: <ul style="list-style-type: none"> • can be repeated given certain configuration in the target • can be repeated with minimal customisation of the published exploits (e.g. change of parameters)
Possible (3)	The vulnerability of the target: <ul style="list-style-type: none"> • can be discovered by examining the target's responses, behaviour and communications (e.g. fuzzing with network packets, network sniffing); • can be discovered and attacked from within the same subnet or network segment 	The attack: <ul style="list-style-type: none"> • can be performed with privilege access rights of the target (e.g. admin/SYSTEM/root) • can be performed with publicly available tools that requires moderate technical knowledge 	The attack: <ul style="list-style-type: none"> • can be repeated given certain predictable event condition • can be repeated with customisation specific for the target
Unlikely (2)	The vulnerability of the target: <ul style="list-style-type: none"> • can be discovered by operating and interacting with the 	The attack: <ul style="list-style-type: none"> • can be performed with privilege access rights (e.g. admin/SYSTEM/root); 	The attack: <ul style="list-style-type: none"> • can be repeated given certain random event condition

¹⁰ Configuration refers to settings in a hardware, software or firmware that can be changed, affecting the security posture and/or functionality of the system. For example, the enabling of Telnet service.


¹¹ Event condition refers to a situation/circumstance of the computing environment that must exist to achieve the desired outcome. For example, an ad-hoc batch job needs to be running in order for the attack to be carried out.

Likelihood Rating	Discoverability	Exploitability	Reproducibility
	<p>actual or similar setup of the target;</p> <ul style="list-style-type: none"> can be discovered and attacked with logical local access 	<ul style="list-style-type: none"> can be performed with publicly available/specialise tools that requires advance technical knowledge may requires chaining of multiple exploits 	<ul style="list-style-type: none"> can be repeated theoretically or with published proof of concept exploit
Rare (1)	<p>The vulnerability of the target:</p> <ul style="list-style-type: none"> can be discovered by studying the blueprint (e.g. source code) can be discovered and attacked with physical access 	<p>The attack:</p> <ul style="list-style-type: none"> can be performed with privileged access rights (e.g. admin/root/SYSTEM) and required multi-factor authentication; can be performed with specialised tools that requires expert technical knowledge requires chaining of multiple exploits 	<p>The attack:</p> <ul style="list-style-type: none"> cannot be reproduced on the target can be repeated with unpublished exploit specific for the target

Figure 3: A sample assessment table for determining risk likelihood

CIIOs to note:

In the CII risk assessment report,



- The risk likelihood must be scored along the scale of 1 to 5 (i.e. 1 being “rare” and 5 being “highly likely”) ¹².
- The risk likelihood must be determined based on threat and vulnerability.
- The likelihood factors (i.e. Discoverability, Exploitability, and Reproducibility) are recommended for use to determine the risk likelihood.

¹² Consistency in the use of risk likelihood scale is necessary, so that CII risks can be aggregated and viewed at the national level.

Task B: Determine Impact

In general, the manifestation of a risk scenario can compromise the confidentiality, integrity and/or availability of assets (e.g. data, equipment, operations). Any compromise of the assets will translate to adverse impact at the following three (3) levels:

- **National** – At the national level, the impact can be viewed as harm to national security and economy.
- **Organisational** – At the organisational level, the impact can be viewed as disruption to business operations, damage to reputation and loss of financials.
- **Individual** - At the individual level, the impact can be viewed as loss of life and injuries.

Figure 4 below is a sample assessment table for determining the risk impact on a rating scale of 1 to 5 (5 being “Very Severe” and 1 being “Negligible”). The descriptors provided in the sample table below are generic. When adopting a similar impact table, organisations should review and tailor the descriptors for each impact rating to ensure they are:

- **Relevant to business context** - Link descriptors to the organisation’s business objectives or performance measures.
- **Unambiguous** - Use descriptors that are binary or with quantitative ranges (e.g. leakage of data classified as “Confidential”, disruption of services to more than 50% of customers)
- **Multi-perspectives** - Identify sub-categories of impact from each of the 3 levels (i.e. national, organisational, and individual)

Impact Rating	Confidentiality	Integrity	Availability
Very Severe (5)	The unauthorised disclosure of information could be expected to have an exceptionally grave adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>	The unauthorised modification or destruction of information could be expected to have an exceptionally grave adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>	The disruption of access to or use of information or computer system could be expected to have an exceptionally grave adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>
Severe (4)	The unauthorised disclosure of information could be expected to have a serious adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>	The disruption of access to or use of information or computer system could be expected to have a serious adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>


Impact Rating	Confidentiality	Integrity	Availability
Moderate (3)	The unauthorised disclosure of information could be expected to have some adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>	The unauthorised modification or destruction of information could be expected to have some adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>	The disruption of access to or use of information or computer system could be expected to have some adverse effect on <u>organisation</u> , <u>individuals</u> , or the <u>nation</u>
Minor (2)	The unauthorised disclosure of information could be expected to have a limited adverse effect on <u>organisation</u> , or <u>individuals</u>	The unauthorised modification or destruction of information could be expected to have a limited adverse effect on <u>organisation</u> , or <u>individuals</u>	The disruption of access to or use of information or computer system could be expected to have a limited adverse effect on <u>organisation</u> , or <u>individuals</u>
Negligible (1)	The unauthorised disclosure of information could be expected to have negligible effect on <u>organisation</u> , or <u>individuals</u>	The unauthorised modification or destruction of information could be expected to have negligible effect on <u>organisation</u> , or <u>individuals</u>	The disruption of access to or use of information or computer system could be expected to have negligible effect on <u>organisation</u> , or <u>individuals</u>

Figure 4: Generic descriptors for determining impact of risk

Each risk scenario may be assessed to have different impact ratings in areas of confidentiality, integrity and availability. The highest impact rating should be taken as the final score.

CIIOs to note:

In the CII risk assessment report,



- The risk impact must be scored along the scale of 1 to 5 (1 being “negligible” and 5 being “very severe”)¹³.
- The descriptors for each impact rating must be tailored to respective organisational context.

¹³ Consistency in the use of risk impact scale is necessary, so that CII risks can be aggregated and viewed at the national level.

4.3 Step 3: Risk Evaluation

Risk evaluation is about determining and understanding the significance of risk level, and comprises the following tasks:

- Determine and prioritise risk
- Document risk

Task A: Determine and Prioritise Risk

As mentioned in *Chapter 3*, risk is a function of the likelihood of a given threat event exploiting a potential vulnerability of an asset, and resulting impact. This can be diagrammatically presented using a risk matrix. *Figure 5* below is a sample 5-by-5 risk matrix for determining risk level for each risk scenario, where risk level is a multiplication of “Likelihood” and “Impact” determined from the Risk Analysis step (Section 4.2).

IMPACT	Very Severe (5)	Medium (5)	Medium High (10)	High (15)	Very High (20)	Very High (25)
	Severe (4)	Low (4)	Medium (8)	Medium High (12)	High (16)	Very High (20)
	Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium High (12)	High (15)
	Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium High (10)
	Negligible (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Highly Likely (5)	
	LIKELIHOOD					

Figure 5: A 5-by-5 Risk Matrix for determining risk level

For each risk level derived, compare it against the risk tolerance level defined by the organisation. Risk scenarios with risk levels above the tolerance level must be prioritised for treatment until the risk levels fall to within the tolerance level. When prioritising risk for treatment, the expected duration should also be established.

**CIIOs to note:**

In the CII risk assessment report, the risk level must be determined using a 5-by-5 matrix and along a scale of 1 to 5 (1 being “low” and 5 being “very high”)¹⁴.

Task B: Document Risk

A risk assessment is incomplete without documentation. The outputs from previous steps must be clearly documented in a Risk Register for communication to stakeholders. A Risk Register is a record of all the risk scenarios identified, including their determined risk level. The Risk Register is a living document to be regularly reviewed and updated to ensure that the organisation’s management has an up-to-date picture of the organisation’s cybersecurity risks when making risk-informed decisions. It should minimally contain the following:

- **Risk scenario** – A scenario articulating how a threat event could exploit a potential vulnerability of an asset to create an adverse impact.
- **Identification date** – The date when the risk scenario is identified.
- **Existing measures** – The current measures in place to address the risk scenario.
- **Current risk** – The determined risk level (combination of likelihood and impact) of risk scenario after taking into account existing measures (i.e. inherent risk¹⁵ with existing measures applied).
- **Treatment plan** – The planned activities (e.g. deploying additional measures) and timeline to treat the current risk to an acceptable level (i.e. within organisation’s risk tolerance level).
- **Progress Status** – The status of implementing the treatment plan.
- **Residual risk** – The determined risk level (combination of likelihood and impact) of risk scenario after treatment plan is implemented (i.e. current risk with additional measures applied).
- **Risk Owner** – The individual or group responsible for ensuring that the residual risks remain within the organisation’s tolerance level.

**CIIOs to note:**

In the CII risk assessment report, the Risk Register must minimally include the eight (8) elements, namely *risk scenario*, *identification date*, *existing measures*, *current risk*, *treatment plan*, *progress status*, *residual risk*, *risk owner*.

¹⁴ Consistency in the use of risk matrix is necessary, so that CII risks can be aggregated and viewed at the national level.

¹⁵ Inherent risk refers to risk level without taking into account any measures.

5 RESPOND TO RISKS

Having evaluated the identified risks (i.e. current risks), the next step is to identify and determine the next course of action to keep the risks within the organisation's risk tolerance level.

5.1 Types of Risk Response Options

There are four (4) risk response options to consider:

Accept

Risk acceptance means undertaking risk as it is without introducing further actions to reduce it. Risk should only be accepted when it falls within the organisation's tolerance level.

Avoid

Risk avoidance means discontinuing an action/activity that exposes the organisation to the identified risk. This may appear extreme but may be the best course of action if the risk outweighs the benefits.

Example: Not conducting online payment transactions is an example of avoiding the risk of attackers hijacking the transaction to make fraudulent payments.

Transfer

Risk transference means sharing a portion of risk with other parties or entities. Such a treatment option typically reduces the "impact" component of risk.

Example: Purchasing cyber insurance or outsourcing certain operations are examples of sharing risks with third parties.

Mitigate

Risk mitigation means putting in place measures to reduce the risk level. This can be achieved through the deployment of security controls.

Example: Implementing a firewall to restrict network traffic is an example to mitigate the risk of system communicating with malicious external servers.

Whichever risk response option is taken, senior management (with the appropriate level of authority and accountability) within the organisation must formally approve the selected risk response and make a conscious decision to accept the residual risks.

5.2 Choosing the Appropriate Risk Response Actions

Many organisations tend to treat risks through mitigation by investing in costly security controls and technical solutions. However, organisations should also explore treating risks through avoidance or transference as possible alternatives that may also be cost-effective. For example, in order to address the risk of system compromise when employees access malicious websites, organisations may want to consider avoiding the risk by removing internet-surfing capabilities instead of mitigating the risk through deployment of expensive end-point preventive solutions.

When organisations choose to treat risks through mitigation, they need to ensure that the security controls they implement are relevant and appropriate to the risks they are addressing. As a general guidance, a control is considered appropriate and relevant to a risk when it:

- Reduces risk likelihood; or
- Reduces risk impact

CIIOs to note:




In the CII risk assessment report,

- Senior Management must formally approve all treatment plans.
- Senior Management must formally accept all residual risks.

6 REFERENCES

- [1] J. T. Langill and E. D. Knapp, *Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Elsevier, 2014.
- [2] C. E. Bodungen, B. L. Singer, A. Shbeeb, S. Hilt and K. Wilhoit, *Industrial Control Systems Hacking Exposed*, McGraw-Hill Education, 2017.
- [3] (NIST), National Institute of Standards and Technology, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-39/final>. [Accessed 19 November 2019].
- [4] ISACA, *CRISC Review Manual 6th Edition*, ISACA, 2015.
- [5] Australian Government, Department of Finance, "Comcover Risk Resources - Defining Risk Appetite and Tolerance," 2016. [Online]. Available: <https://www.finance.gov.au/sites/default/files/2019-11/case-study-defining-risk-appetite-and-tolerance.PDF>. [Accessed 19 November 2019].
- [6] A. Shostack, *Threat Modeling: Designing for Security*, John Wiley & Sons Inc., 2014.
- [7] Microsoft, "Chapter 3 - Threat Modeling," 7 July 2010. [Online]. Available: [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644\(v=pandp.10\)](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)). [Accessed 19 November 2019].
- [8] (NIST), National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," September 2012. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>. [Accessed 19 November 2019].
- [9] Paladin Risk Management Services, "Risk Tip #5 - Hungry to Understand Risk Appetite?," 2017. [Online]. Available: <https://paladinrisk.com.au/risk-tip-5-hungry-understand-risk-appetite>. [Accessed 19 November 2019].

Summary of Expectations for CIIOs

 CIIOs to note:	Related Section
In the CII risk assessment report, risk tolerance levels must be clearly defined.	3.2
In the CII risk assessment report, the stakeholders' roles and responsibilities in the risk assessment exercise must be clearly specified.	3.3
In the CII risk assessment report, risk scenarios must include elements of threat event, vulnerability, asset and consequence.	4.1
In the CII risk assessment report, <ul style="list-style-type: none"> • The risk likelihood must be scored along the scale of 1 to 5 (<i>i.e. 1 being "rare" and 5 being "highly likely"</i>). • The risk likelihood must be determined based on threat and vulnerability. • The likelihood factors (<i>i.e. Discoverability, Exploitability, and Reproducibility</i>) are recommended for use to determine the risk likelihood. 	4.2 [Task A]
In the CII risk assessment report, <ul style="list-style-type: none"> • The risk impact must be scored along the scale of 1 to 5 (<i>1 being "negligible" and 5 being "very severe"</i>). • The descriptors for each impact rating must be tailored to respective organisational context. 	4.2 [Task B]
In the CII risk assessment report, the risk level must be determined using a 5-by-5 matrix and along a scale of 1 to 5 (<i>1 being "low" and 5 being "very high"</i>).	4.3 [Task A]
In the CII risk assessment report, the Risk Register must minimally include the eight (8) elements, namely <i>risk scenario, identification date, existing measures, current risk, treatment plan, progress status, residual risk, risk owner</i> .	4.3 [Task B]
In the CII risk assessment report, <ul style="list-style-type: none"> • Senior Management must formally approve all treatment plans. • Senior Management must formally accept all residual risks. 	5.2

QUERIES & FEEDBACK

Questions and feedback on this document may be submitted to:

CII_Supervision@csa.gov.sg