Digital Policy Office

INFORMATION SECURITY

Practice Guide

for

IT Security Risk Management

Version 1.1

July 2024

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
1	Change “Office of the Government Chief Information Officer” (or “OGCIO”) to “Digital Policy Office” (or “DPO”)		1.1	July 2024

Table of Contents

1. Introduction

IT security risk management is an essential process that helps organisations proactively identify, assess, and prioritise potential IT security risks that may impact their objectives. This document rprovides a reference model to align IT security risk management practices and methodologies. By referencing this model, managerial users, IT managers, system administrators, and other technical and operational staff can better understand the IT security risk management process. They will be able to grasp the necessary preparations, key considerations, and achievable outcomes. The objective of this document is to provide a comprehensive framework for Bureaus and Departments (B/Ds) to implement effective and customised IT security risk management practices that suit their specific needs and context.

1.1 Purpose

This document describes a general framework for IT security risk management. It should be used in conjunction with other security documents such as the Baseline IT Security Policy [S17], IT Security Guidelines [G3] and relevant procedures, where applicable.

This practice guide is intended for all staff who are involved in IT security risk management as well as for the IT security consultants or auditors who support the IT security risk management process for the Government.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of the Hong Kong Special Administrative Region.
- IT Security Guidelines [G3], the Government of the Hong Kong Special Administrative Region.
- Information security, cybersecurity and privacy protection – Information security management systems – Requirements, ISO/IEC 27001:2022.
- Information security, cybersecurity and privacy protection – Information security controls, ISO/IEC 27002:2022.
- Information security, cybersecurity and privacy protection – Guidance on managing information security risks, ISO/IEC 27005:2022.
- Risk Management – Guidelines, ISO 31000:2018.
- NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM).

- NISTIR 8286A Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management.
- NISTIR 8286B Prioritizing Cybersecurity Risk for Enterprise Risk Management.
- NISTIR 8286C Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight.
- GB /T 31722-2015 Information Technology - Security Techniques - Information Security Risk Management.
- GB/T 20984-2022 Information Security Technology - Risk Assessment Method for Information Security.
- GB/T 24353-2022 Risk Management - Guidelines.
- GB/T 22080-2016 Information Technology - Security Techniques - Information Security Management Systems - Requirements.
- Practice Guide for IT Security Threat Management
- Practice Guide for Security Risk Assessment and Audit

1.3 Definitions and Conventions

For the purposes of this document, the definitions and conventions given in S17, G3, and the following shall apply.

Abbreviation and Terms	
IT Security	IT security is the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring the confidentiality, integrity, and availability of information.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
IT Security Risk Management	The continuous process of identifying, prioritising, mitigating and controlling potential IT security risks associated with human and/or operation problems to an acceptable and manageable level.
Stakeholder	Personal or organisation that can be affected by, or perceive themselves to be affected by, a decision or activity.

1.4 Contact

This document is produced and maintained by the Digital Policy Office (DPO). For comments or suggestions, please send to:

Email:	it_security@digitalpolicy.gov.hk
Lotus Notes mail:	IT Security Team/DPO/HKSARG@DPO
CMMP mail:	IT Security Team/DPO

2. Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include but not limited to the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audit on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone’s business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of threat intelligence platforms to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

Staff may also raise their security awareness by participating security drills, attending seminars, showcases or visiting theme pages containing security intelligence information and general security information (e.g. Cyber Security Information Portal, InfoSec website).

3. IT Security Risk Management

3.1 Introduction to IT Security Risk Management and its Importance

IT security risk relates to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems. It reflects potential adverse impacts on organisational operations (i.e., mission, functions, image, or reputation), assets, individuals, other organisations, and society.

Effective IT security risk management is a vital process that involves identifying, assessing, and mitigating risks to an organisation's information systems, data, and technology infrastructure and identifying vulnerabilities and threats that could compromise the confidentiality, integrity, and availability of digital assets. Implementing robust strategies is necessary to mitigate these risks to an acceptable level defined by the organisation.

In the digital age, IT security risk management is crucial in safeguarding sensitive information, critical infrastructure, and business continuity. Due to the increasing reliance on technology, the prevalence of potential risks and vulnerabilities associated with IT threats has grown. By implementing robust risk management practices, B/Ds can proactively identify and address potential security gaps and achieve the following objectives:

- Protect valuable assets, such as sensitive data, intellectual property, customer information, and critical systems.
- Enhance visibility of potential IT security risks, enabling better resource allocation and decision-making.
- Provide management with a comprehensive and systematic view of existing IT security risk profiles and corresponding security safeguards.
- Reduce the likelihood and impact of IT security incidents while maintaining business continuity.
- Ensure compliance with relevant IT security legislation and regulatory requirements, avoiding potential legal penalties and reputational damage.

Inadequate risk management can have significant consequences for B/Ds. For example, data breaches can lead to the unauthorised disclosure of sensitive information, resulting in legal and regulatory repercussions. Furthermore, the loss or compromise of critical data may disrupt essential government services, undermining public trust and confidence.

3.2 IT Security Risk Management Framework

To ensure consistency and effectiveness in IT security risk management, B/Ds shall formulate a comprehensive IT security risk management framework that outlines how risks related to B/Ds and their systems are identified, assessed, mitigated, and monitored. A reliable framework provides a structured approach to managing IT security risks. It facilitates a comprehensive understanding of potential threats and vulnerabilities. By adhering to a framework, B/Ds can strengthen their IT security posture and effectively manage their IT security risks.

An IT risk management framework aims to provide a structured approach through a series of risk management activities and functions. The effectiveness of IT security risk management depends on its integration into the governance of B/Ds, including decision-making. This requires support from stakeholders, particularly top management. The below figure illustrates the key components of the framework.

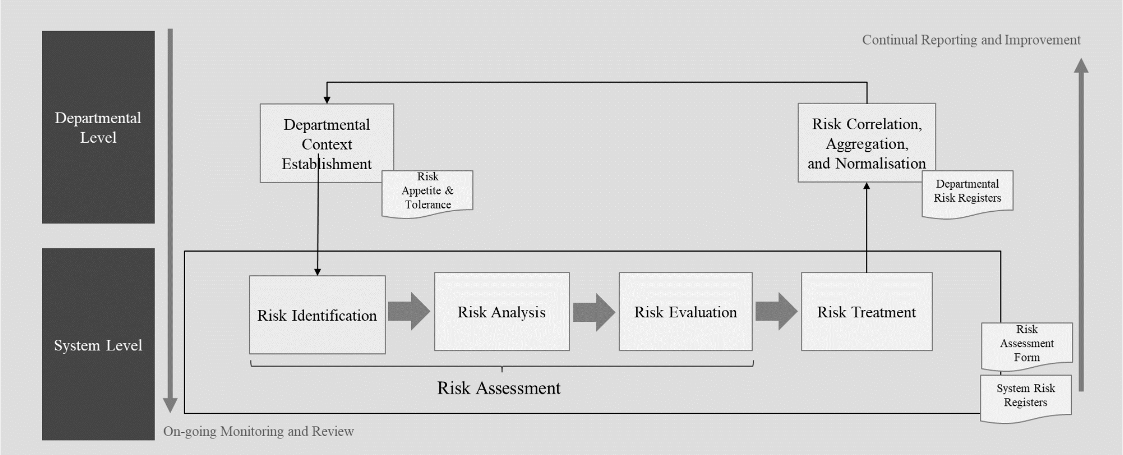
Departmental Level
System Level
Continual Reporting and Improvement
Departmental Context Establishment
Risk Appetite & Tolerance
Risk Correlation, Aggregation, and Normalisation
Departmental Risk Registers
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
Risk Assessment
Risk Assessment Form
System Risk Registers
On-going Monitoring and Review

Figure 3.1 IT Security Risk Management Framework

(i) Department Context Establishment (Section 3)
Understanding and defining the internal and external context of the B/D can influence the overall management of IT security risks.

(ii) Risk Identification (Section 4)
Identifying and documenting potential IT security threats and vulnerabilities that could impact the B/D's information systems and data.

(iii) Risk Analysis (Section 4)
The identified risks are further analysed to understand their potential impact and likelihood. This provides a comprehensive understanding of the potential impact of each risk on the B/D's operations and objectives.

(iv) Risk Evaluation (Section 4)

Comparing the analysed risks against the B/D’s risk criteria to prioritise them. It helps determine the significance of each risk and decide which risks need to be treated.

(v) Risk Treatment (Section 4)
After evaluating risks, appropriate treatment options are developed to manage them. This could involve avoiding the risk, transferring it, mitigating it through controls, or accepting it, depending on the B/D’s risk appetite.

(vi) Risk Correlation, Aggregation and Normalisation (Section 5)
Examining the interrelationship between risks, combining and assessing their overall impact, and standardising risk measurements. This gives a more holistic understanding of the B/D’s risk environment and helps inform strategic decision-making.

The iterative approach can increase the depth and detail of the assessment at each iteration, balancing the time and effort spent identifying controls and ensuring that risks are appropriately assessed.

3.3 IT Security Risk Management Policy

An IT security risk management policy should be established as a formal IT security management framework document to outline the B/D's business objectives, the threats they need to protect against, and any applicable legal and regulatory requirements. The IT security risk management policy should also provide a top-down perspective of what needs to be protected and the B/D will not tolerate any behaviour or acts of non-comformance. When establishing an IT security risk management policy, B/D should refer to this Practice Guide and determine its risk management approach, such as the risk assessment methodology, risk rating calculation mechanism, and Key Performance Indicators (KPIs), in accordance with its strategy and objectives. The policy provides requirements and guidance on how the B/D should protect its information assets, systems, and networks from potential threats and vulnerabilities. While the specifics of the policy may vary depending on the B/D's size, complexity, industry, and regulatory requirements, here are some common elements that are typically included in an IT security risk management policy:

- Purpose and scope
- Roles and responsibilities
- Formulation and execution of its security risk management framework within a B/D
- Compliance and enforcement
- Training and Awareness
- Policy Review and Approval

B/Ds should develop their respective standards and guidelines to supplement their own policy.

4. Departmental Context Establishment

Departmental context establishment customises the risk management process, enabling effective risk assessment and appropriate risk treatment for a B/D.

4.1 Defining Risk Management Scope

Defining the scope of IT security risk management activities in each B/D is paramount.

A clear scope ensures targeted and effective risk management efforts. This involves creating a comprehensive inventory of the information systems and their components subject to risk assessment. This information should be documented in an information system inventory list. The scope should include a Network Diagram or System Architecture Diagram that visually represents the connections within and outside the system, the extent of control the B/D has on these systems and any external systems or services these systems rely on.

Defining the risk management scope is crucial to understanding dependencies on other government entities or other external stakeholders, facilitating collaboration and coordination in addressing IT security risks across different domains.

It is essential to clearly define the scope, considering the following aspects:

- Objectives and decisions to be made.
- Expected outcomes from the process steps.
- Time, location, specific inclusions, and exclusions.
- Appropriate risk assessment tools and techniques.
- Required resources, responsibilities, and record-keeping.
- Relationships with other projects, processes, and activities.

By establishing a well-defined scope, B/Ds can enhance their IT security risk management practices in line with industry best practices and effectively address potential risks.

4.2 Understanding Risk Context

B/Ds operate within a unique risk context shaped by their objectives, assets, threats, vulnerabilities, and legal/regulatory requirements. Thoroughly assessing and understanding this specific risk context is crucial for B/Ds. By considering these factors, valuable insights into potential risks can be gained, enabling tailored risk management strategies to be devised. B/Ds should gather information to consider and understand the external and internal context.

Factors of external context may include, but not be limited to, the following examples:

- Social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local.
- Key drivers and trends affecting the objectives of B/Ds.
- External stakeholders' relationships, perceptions, values, needs and expectations.
- Contractual relationships and commitments.
- The complexity of networks and dependencies.

Factors of internal context may include, but not be limited to, the following examples:

- Vision, mission and values.
- Governance, structure, roles and accountabilities.
- Strategy, objectives and policies.
- Culture.
- Standards, guidelines and models adopted by B/Ds.
- Capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, intellectual property, processes, systems and technologies).
- Data, information systems and information flows.
- Relationships with internal stakeholders, taking into account their perceptions and values.
- Contractual relationships and commitments.
- Interdependencies and interconnections.

4.3 Defining Risk Appetite Statement and Risk Tolerance Criteria

Risk appetite statement and risk tolerance criteria are vital in decision-making within the B/D's IT security risk management framework. They help establish acceptable levels of risk and guide the prioritisation of risk mitigation efforts. It is important that they are aligned with the risk management framework and tailored to the specific purpose and scope of the activity being considered. They should reflect the B/D's values, objectives, and resources and be consistent with policies and guidelines on IT security risk management.

Risk appetite defines the level of risk the B/D is willing to accept in pursuit of its objectives. In contrast, risk tolerance sets the threshold beyond which risks are considered unacceptable. B/Ds should determine their risk appetite statements and risk tolerance criteria in the IT security risk management policy to establish a strategic approach to risk management. It is essential to establish these statements early on and reassess them periodically to ensure they align with the evolving objectives and risk environment of the B/D.

Defining risk appetite statements and risk tolerance criteria should consider the B/D's obligations and stakeholders' views. While risk appetite statement and risk tolerance criteria should be established at the beginning of the risk assessment process, they should be regularly reviewed and amended, if necessary.

To set risk appetite statement and risk tolerance criteria, the following factors should be considered:

- The nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible).
- How impact (both positive and negative) and likelihood are defined and measured.
- Time-related factors.
- Consistency in the use of measurements.
- How the level of risk is to be determined.
- How combinations and sequences of multiple risks are taken into account.
- The B/D's capacity.

4.3.1 Risk Appetite

Risk appetite reflects the B/D's willingness to take risks in line with its objectives, strategic goals, priorities, and risk culture. A high risk appetite means the B/D is willing to take more risks to achieve its objectives, while a low risk appetite means the B/D prefers to take fewer risks. Risk appetite may be qualitative or quantitative. B/Ds should align their IT security strategies with the defined risk appetite, setting a tone that promotes security consciousness and risk awareness within their respective departments. It allows B/Ds to balance innovation and risk mitigation, ensuring risks are managed within acceptable limits. By establishing a clear risk appetite, the B/D creates a framework to assess and respond to risks, guiding decision-making processes and aligning with overall goals. Whether qualitative or quantitative, the risk appetite sets boundaries for risk-taking, considering potential benefits and negative impacts. Defining the risk appetite enables a consistent and informed approach to risk management at the departmental level.

Risk Appetite Examples:

- Organisation has an amber threshold of 0.2% downtime of critical systems.
- Organisation has a red threshold for 2 or more negative media reports from a given Country Office.
- Organisation has a high risk appetite for in-country supply chain risks.
- Organisation has a high risk appetite for investing in areas that could provide significant improvement and innovation in its operations.
- Organisation has a low risk appetite for reputational risks or potential conflicts of interest.

B/Ds should consider several factors to ensure a comprehensive and informed approach when determining the risk appetite. These factors play a crucial role in shaping the risk appetite and guiding decision-making processes:

- Strategic Objectives: The risk appetite should align with the B/D's strategic objectives and mission/vision. B/Ds should evaluate how much risk the B/D is willing to take to achieve those objectives and carefully assess the potential impact on the organisation's long-term goals.

- Risk Culture: The organisation's risk culture should be considered, including its attitude towards risk-taking and willingness to embrace innovative initiatives or adopt more conservative approaches.
- Stakeholder Expectations: The expectations and preferences of various stakeholders, such as the government, regulatory bodies, customers, and the public, should be considered. Understanding stakeholder perspectives on risk is crucial in shaping the risk appetite to maintain trust and meet societal expectations.
- Legal and Regulatory Requirements: Compliance with applicable laws, regulations, and industry standards is paramount. B/Ds should consider the legal and regulatory obligations related to risk management and ensure that the risk appetite is set within the boundaries established by these requirements.
- Industry and Market Conditions: The B/D's industry and market conditions should influence the risk appetite. B/Ds should assess the competitive landscape, market volatility, emerging risks, and industry best practices to determine an appropriate risk appetite.
- Financial Capacity: The B/D's financial capacity to bear and manage risks should be carefully evaluated. B/Ds should consider the organisation's financial resources, risk tolerance in relation to financial implications, and the potential impact on stakeholders, including shareholders and investors.
- Organisational Resilience: The B/D's ability to withstand and recover from adverse events should be considered. B/Ds should assess the organisation's resilience capabilities and determine how much risk it can reasonably take without compromising its ability to respond and recover effectively.

4.3.2 Risk Tolerance

Risk tolerance refers to the acceptable level of performance variation in relation to achieving objectives. Risk tolerance is generally established at the program, objective, or component level. B/Ds should interpret their risk appetite to develop specific IT security risk tolerance levels within the B/D while ensuring that these levels are consistent with overall objectives and legal or regulatory requirements.

Defining risk tolerance is crucial as it sets the boundaries for risk-taking and guides the implementation of control and mitigation measures. B/Ds can effectively manage IT security risks within predefined limits by establishing clear risk tolerance thresholds. This ensures that resources are prioritised towards critical areas and enables B/Ds to allocate risk treatment efforts appropriately. A well-defined risk tolerance enhances decision-making and facilitates efficient IT security risk management resource allocation.

Risk Tolerance Example:
The B/D will not accept any risk arising from a "High Risk" event after mitigation under any circumstances. Meanwhile, the B/D will not accept any risk arising from a "Medium Risk" event after mitigation unless approved by the DITSO.

To establish clear risk tolerance thresholds for managing IT security risks, B/Ds should consider the following factors:

- Key Objectives: B/D should identify its key objectives. This typically involves the information systems that need protection from IT security risks.
- Stakeholders Consultation: It is important to consult relevant stakeholders, such as senior management, legal and compliance teams, IT departments, and external experts, to gather input and ensure that risk tolerance thresholds are comprehensive and practical.
- Regulatory Requirements and Industry Best Practice: B/Ds should stay informed about regulatory requirements and industry best practices related to IT security risk management, which can provide guidance on risk tolerance thresholds.
- Regular Monitoring and Review: Risk tolerance thresholds should be regularly monitored and reviewed to ensure their ongoing relevance and effectiveness. As the IT threat landscape evolves, B/Ds should adapt its risk tolerance thresholds accordingly and implement necessary adjustments to its risk management strategies.

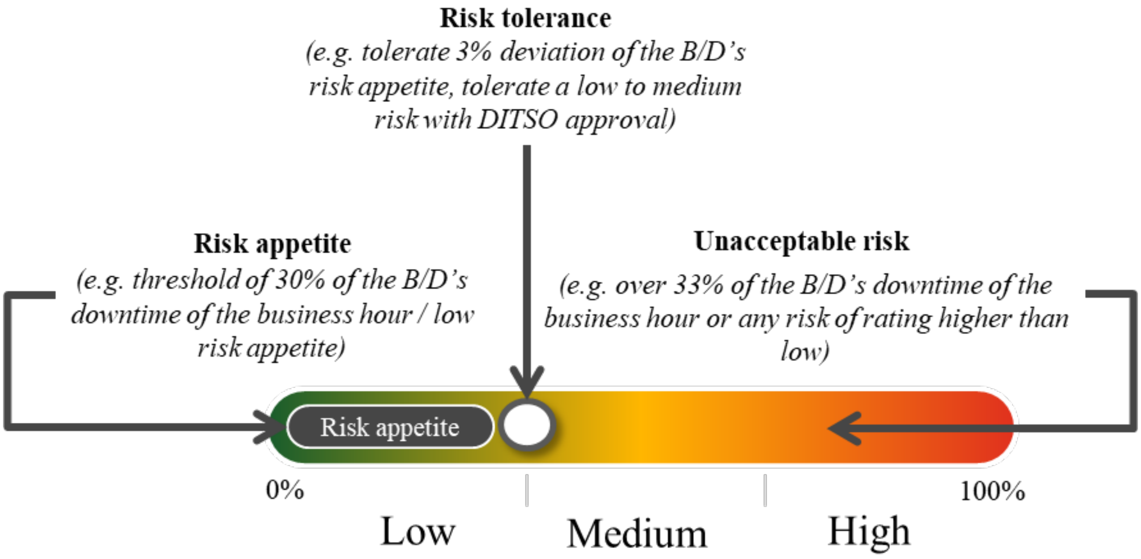
Risk tolerance
(e.g. tolerate 3% deviation of the B/D's risk appetite, tolerate a low to medium risk with DITSO approval)
Risk appetite
(e.g. threshold of 30% of the B/D's downtime of the business hour / low risk appetite)
Unacceptable risk
(e.g. over 33% of the B/D's downtime of the business hour or any risk of rating higher than low)
Risk appetite
0%
100%
Low
Medium
High

Figure 4.1: Illustration of risk appetite, risk tolerance, and uncceptable risk

4.4 IT Security Risk Coordination, Integration and Reporting

Coordinating and integrating IT security risk management efforts within the B/D is crucial for a holistic approach to risk mitigation. B/Ds should establish processes for coordination and integration, ensuring that risk management activities are aligned with the overall goals. This includes fostering collaboration among relevant teams, units, and stakeholders to share information, best practices, and lessons learnt. Additionally, robust reporting mechanisms should be established to ensure transparency, accountability, and timely communication of IT security risks. Regular reporting on risk status and mitigation progress enables informed decision-making at all levels of the B/D.

The IT security risk coordination, integration, and reporting should be implemented as part of the B/D's overall risk management framework and processes. It should be established early in risk management planning and continuously reviewed and updated to align with changing objectives, risks, and B/D requirements.

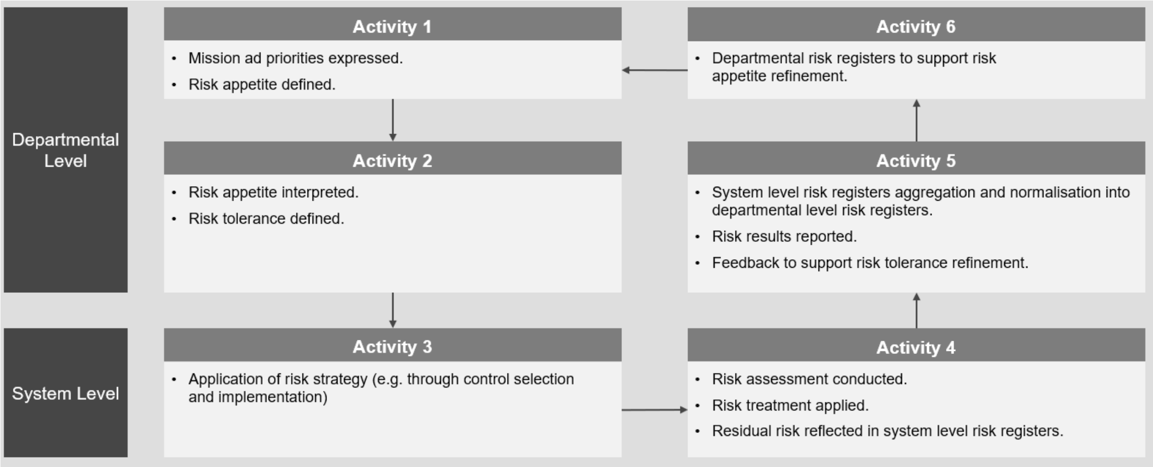
Departmental Level
System Level
Activity 1
• Mission ad priorities expressed.
• Risk appetite defined.
Activity 2
• Risk appetite interpreted.
• Risk tolerance defined.
Activity 3
• Application of risk strategy (e.g. through control selection and implementation)
Activity 4
• Risk assessment conducted.
• Risk treatment applied.
• Residual risk reflected in system level risk registers.
Activity 5
• System level risk registers aggregation and normalisation into departmental level risk registers.
• Risk results reported.
• Feedback to support risk tolerance refinement.
Activity 6
• Departmental risk registers to support risk appetite refinement.

Figure 4.2: Illustration of Risk Coordination, Integration and Reporting

4.5 Roles and Responsibilities

B/Ds should identify the key roles involved in IT security risk management and define the responsibilities, reporting lines, and accountabilities for each role. B/Ds should assign individuals to each role based on their knowledge, experiences, and understanding of the systems and processes involved. IT security roles and responsibilities should be defined during the planning or implementation phase of the risk management framework. It is essential to establish these roles and responsibilities early on and periodically review and update them to ensure alignment with changing business objectives and risk environment.

Roles and responsibilities should cover all levels of staff, from senior management, who sets the risk appetite and tolerance, to operational staff implementing risk treatment measures.

At the B/D level, roles include strategic decision-makers and those overseeing the overall risk management framework. These roles should have a broad perspective and understanding of the B/D's business objectives, risk appetite, and risk tolerance. They should be responsible for setting the B/D's IT security risk framework and ensuring alignment with the B/D's mission and vision.

At the system level, roles might include the risk owner, who manages specific information systems and implements risk mitigation measures. These roles should have a detailed understanding of the particular systems and the risks identified.

4.5.1 Risk Owner

Risk owner is the individual or functional unit entrusted with the accountability and authority to manage risk. The risk owner may hold positions as process owners, functional owners, project managers, or asset owners; or come from senior management or the security committee. B/Ds should utilise the risk assessment process or establish criteria for identifying risk owners. Please refer to Practice Guide for Security Risk Assessment and Audit for details. When identifying risk owners, the following factors should be taken into consideration:

- The level of risk and the asset to which the risk pertains.
- The accountability and authority required for managing the risks.
- Understanding the issues and the ability to make well-informed decisions (e.g., determining how to mitigate the risks).

The example responsibilities of a risk owner are provided below for reference.

- Identifying and assessing potential IT security risks.
- Developing and implementing appropriate strategies and safeguards to mitigate risks.
- Monitoring the status of identified IT security risks and the effectiveness of risk mitigation plans.
- Communicating risk-related information, policies, and procedures to stakeholders within their area of responsibility.
- Reporting IT security risks to senior management and DITSO.

5. IT Security Risk Assessment and Treatment

The IT security risk assessment process should encompass identifying, analysing and evaluating internal and external risks. Internal risks refer to vulnerabilities and threats within the B/D, such as technological weaknesses, operational gaps, and human-related factors, including human error or insider threats. On the other hand, external risks include threats originating from outside the B/D, such as IT security attacks, hacking attempts, and emerging threat vectors.

Identifying and assessing internal risks is crucial as it helps uncover potential weaknesses and vulnerabilities within the B/D's systems, processes, and personnel. This includes evaluating the effectiveness of existing security measures, assessing the robustness of technical controls, and identifying any operational gaps that malicious actors could exploit. Additionally, understanding human-related factors, such as employee awareness, training, and adherence to security protocols, is essential in mitigating risks within the B/D.

Equally important is the identification and assessment of external risks. This involves analysing the threat landscape and staying informed about emerging IT threats and attack vectors. By understanding threat actors' tactics, techniques, and procedures, B/Ds can proactively implement appropriate countermeasures and preventive measures. Regular monitoring of external threats and vulnerabilities helps identify potential weaknesses and take prompt action to address them. For more details, please refer to the Practice Guide for IT Security Threat Management.

By considering technological, operational, and human-related factors in the risk assessment process, B/Ds can gain a comprehensive understanding of the IT security risks they face. This holistic approach is important for developing targeted risk mitigation strategies and allocating resources to address identified vulnerabilities effectively. It also helps prioritise risk treatment efforts based on the severity and potential impact of identified risks.

After IT security risks are identified, analysis and prioritisation of such risks should be performed, and B/Ds should choose the appropriate risk treatment options, including **risk acceptance, risk reduction**, **risk avoidance**, and **risk transfer**.

To conduct a thorough and effective IT security risk assessment and treatment process, B/Ds are advised to refer to the **Practice Guide for Security Risk Assessment and Audit**. This guide provides valuable guidance and best practices for identifying, analysing and evaluating IT security risks within information systems of government organisations

At the end of the IT security risk assessment and treatment process, the information that has been gathered and analysed is compiled and documented. The outputs of this process are detailed risk assessment forms and a risk register, which is a list that keeps track of all the risks that have been identified, providing a clear record of what risks exist and how they are being addressed.

6. Risk Correlation, Aggregation, and Normalisation

6.1 Establishing Risk Register

Establishing and maintaining a risk register is critical in effective IT security risk management for B/Ds. The risk register is a central repository for recording identified risks, their likelihood, impact, and associated treatment options. The process begins with the identification and documentation of risks, including both internal and external factors that threaten the B/D’s information systems and operations.

Once risks are identified and assessed, they should be recorded in the risk register, with pertinent details such as risk descriptions, assigned risk owners, current risk levels, and plans for risk treatment. Regular updates to the risk register are essential to reflect changes in the risk environment and the progress of risk treatment activities. By maintaining a comprehensive risk register, B/Ds can gain a comprehensive overview of their risk profiles, facilitating informed decision-making and resource allocation.

After establishing individual system risk registers, B/Ds should consolidate these system level risk registers into a single and comprehensive departmental risk register. The consolidation involves the processes of risk correlation, aggregation, and normalisation. This consolidated register provides a comprehensive overview of all IT security risks within a B/D, providing a holistic perspective of the B/D’s IT security risk environment. The purpose of maintaining a single, integrated departmental risk register is to provide the B/D’s senior management with a clear, organised, and comprehensive view of all the identified IT security risks within the B/D that they need to manage and regularly review, thereby facilitating better planning, resource allocation, and risk treatment. Section 6.2 provides more instructions and examples on consolidating multiple system level risk registers into a departmental risk register.

The departmental risk register should be continuously updated to reflect changes in the risk environment, the effectiveness of controls, or changes in the B/D’s risk strategies. This ensures the departmental risk register remains relevant and useful for informed decision-making regarding IT security risk and proactive risk management.

Annex A shows a template of IT Security Risk Register.

6.2 Performing Risk Correlation, Aggregation, and Normalisation

6.2.1 Risk Correlation

Risk correlation refers to the degree to which the fluctuations or changes in the values of two or more risks are related. It measures the statistical relationships or dependencies between different risks. It indicates how they tend to interact or behave in relation to each other in the risk environment. B/Ds should consider and understand potential interconnections and dependencies between risks across systems. By identifying correlated risks, B/Ds can assess the overall impact of interconnected risks, allocate resources effectively, and implement targeted risk mitigation measures.

It is worth noting that risk correlation can be assessed quantitatively using statistical measures such as correlation coefficients or qualitatively based on expert judgment and historical observations. Risk modelling and simulation techniques can analyse the correlation between risks and simulate their potential impacts on the overall risk profiles. For example, risks in one system may have dependencies or impacts on risks in other areas. By understanding these correlations, risk owners can develop a more comprehensive and integrated approach to risk management.

Risk Correlation Examples:

Assume a B/D has two separate systems: one for customer data management and another for transaction processing. If a vulnerability is identified in both systems that could allow unauthorised access, and if both systems are accessible from the same network, these risks are correlated. An attacker who gains access due to the vulnerability in one system could potentially exploit the same vulnerability in the other system, leading to a more extensive data breach. In this case, the risk owners should ensure sufficient communication and cooperation to develop a holistic approach to manage the correlated risks.

6.2.2 Risk Aggregation

B/Ds should group risks from similar categories across systems to simplify the risk environment and make it easier to understand and manage. The purposes of performing risk aggregation may include, but not be limited to, the followings:

- Consolidating risk information to create a composite IT security risk understanding.
- Enabling adjustment to risk direction (e.g., risk treatment options) to optimise B/D's resource allocation.
- Ensuring monitoring and reporting at various hierarchical levels to maintain situational awareness regarding changes to the risk environment.

Risk aggregation involves combining similar or related risks into a single consolidated risk. This allows B/Ds to view risks on a broader scale and assess their cumulative impact. Aggregated risks provide a clearer picture of the overall risk exposure and enable B/Ds to prioritise mitigation efforts more effectively. Aggregation activities are performed by combining system IT security risk registers with others. The categories (e.g., access control, data security) of each IT security risk in each register are likely to be limited and consistent, so that column provides a practical key for the initial sorting exercise. After all the risks from similar categories at system level are combined, aggregation is a straightforward activity but may require some manual adjustment. Various risk owners will likely use differing risk descriptions for the same scenario. The source of the risk item should be documented to support the ability to trace a risk back to the original register.

Annex B gives some category examples for performing risk aggregation.

Risk Aggregation Examples:

Assuming System A and System B are two systems of a B/D; the two system risk registers will be aggregated into a departmental risk register.

System A risk register

ID	Priority	Risk Description	Risk Category	Likelihood	Impact	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
1	High	An external attacker deploys a remote access tool to exfiltrate the B/D's budget plans, resulting in sensitive data disclosure.	Access Control	2	3	3	High	Risk Reduction	Enforce strong authentication mechanisms, e.g., multi-factor authentication (MFA), for all remote access to sensitive systems.	Employee A	31/12/2024	Open
2	High	Vulnerability is identified in the systems that could allow unauthorised access.	Threat Management	2	3	3	High	Risk Reduction	Apply security patches and updates the system vendors or developers provide to address the identified vulnerability.	Employee A	31/12/2024	Open
3	Medium	Incorrect use of the system, causing system failure	People Security	1	3	3	Medium	Risk Reduction	Provide security awareness training to employees on the correct use of the system.	Employee A	31/12/2024	Open

System B risk register

ID	Priority	Risk Description	Risk Category	Likelihood	Impact	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
1	Low	A flood event enters the first-floor data centre, causing water damage to several database servers and interrupting related business services.	Physical Security	1	2	2	Low	Risk Acceptance	N/A.	Employee B	N/A	Closed
2	Medium	Vulnerability is identified in the systems that could allow unauthorised access.	Threat Management	2	3	2	Medium	Risk Reduction	Apply security patches and updates the system vendors or developers provide to address the identified vulnerability.	Employee B	31/12/2024	Open
3	Low	No incident response planning is conducted for the system, causing service disruption in the event of an incident.	Incident Response & Recovery Planning	2	3	2	Medium	Risk Reduction	Establish incident response and recovery planning.	Employee B	31/12/2024	Open

Departmental risk register												
ID	Priority	Risk Description	Risk Category	Likelihood	Impact	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
System A ID #1	High	An external attacker deploys a remote access tool to exfiltrate the B/D's budget plans, resulting in sensitive data disclosure.	Access Control	2	3	3	High	Risk Reduction	Enforce strong authentication mechanisms, e.g., multi-factor authentication (MFA), for all remote access to sensitive systems.	Employee A	31/12/2024	Open
System A ID #2, System B ID #2 (Note 1)	Medium (Note 2)	Vulnerability is identified in the systems that could allow unauthorised access.	Threat Management	2	3	3, 2	Medium (Note 2)	Risk Reduction	Apply security patches and updates the system vendors or developers provide to address the identified vulnerability.	Employee A, B	31/12/2024	Open
System A ID#3	Medium	Incorrect use of the system, causing system failure	People Security	1	3	3	Medium	Risk Reduction	Provide security awareness training to employees on the correct use of the system.	Employee A	31/12/2024	Open
System B ID#1	Low	A flood event enters the first-floor data centre, causing water damage to several database servers and interrupting related business services.	Physical Security	1	2	2	Low	Risk Acceptance	N/A.	Employee B	N/A	Closed
System B ID#3	Low	No incident response planning is conducted for the system, causing service disruption in the event of an incident.	Incident Response & Recovery Planning	2	3	2	Medium	Risk Reduction	Establish incident response and recovery planning.	Employee B	31/12/2024	Open

Note 1: Similar risk items from different system risk registers are combined into a single consolidated risk item.
Note 2: The disparities of risk priorities and risk ratings are adjusted based on B/D appetite, tolerance and resources.

6.2.3 Risk Normalisation

During the aggregation of system risk registers, B/Ds should ensure that the risk information is normalised. To facilitate meaningful comparisons and decision-making, it is crucial to normalise risk information within the B/D. Normalisation involves establishing a common approach or scale for evaluating and comparing risks across different systems. This ensures that risks are assessed and communicated consistently throughout the B/D. At a minimum, the normalisation process at the higher level (e.g., departmental level risk register) should use the same rating criteria to enable comparison and tracking. This typically includes definitions for measuring impact and likelihood to allow comparability across assessment results. Risk criteria may also describe how time factors, such as risk velocity, should be considered in determining the risk severity. B/Ds should consider the following activities during risk normalisation:

- De-duplicate and combine identical or similar risks: If similar risks related to insider threats are identified, consolidate them into a single risk item. This step enables a comprehensive assessment and implementation of appropriate controls. For example, two similar risks are identified within a B/D, the first risk is “Unauthorized data access by employees to the financial system”, while the second risk is “Malicious actions by employees to the HR system”. Since both risks involve employees accessing different information systems without authorization, they can be consolidated into a single risk item categorized “Access Control”: Unauthorized access to information systems (financial system and HR system) by employees.
- Adjust risks according to B/D’s appetite, tolerance, and sensibilities: Since risk ratings have been established at system and departmental levels, reviewing their collective impact and likelihood and recommending higher or lower risk rating adjustments may be necessary. For example, a B/D places a high value on pushing boundaries and embracing technological advancements. However, it has a lower tolerance for risks associated with third-party vendor management. Therefore, the multiple risks related to a specific critical third-party vendor are adjusted to reflect the B/D’s higher concerns.
- Resolve IT security risk register disparities: For example, if there are different risk ratings and risk treatment options assigned to identical or similar risks, the risk owners should communicate with each other and decide to (1) indicate both risk ratings and risk treatment options in the consolidated risk item; or (2) consider to adjust the risks with the same risk rating and same risk treatment option if the risks can be treated and tracked together.
- Adjudicate Key Risks: For example, responsible management highlights and reviews the high risks related to critical systems that supporting a B/D’s business continuity, and these risks need to be tracked and further communicated in the departmental level IT security risk register.

Through normalisation, the results derived from the various system IT security risk registers support consistent risk treatment and communication. Additionally, B/Ds should identify and address disparities in risk treatment among system risk registers, mainly when risk owners treat similar scenarios differently. While variations may exist due to diverse contexts and circumstances, understanding the underlying causes and acknowledging disparities is important. By engaging in collaborative discussions, involving relevant risk owners, and seeking alignment in risk treatment options, B/Ds can promote consistency and fairness in their IT security risk management practices.

Risk Normalisation Examples:

System C risk register

ID	Priority	Risk Description	Risk Category	Likelihood	Impact	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
1	Low	Employees use shared accounts to access the system.	Access Control	2	2	2	Low	Risk Acceptance	N/A.	Employee C	N/A	Closed

System D risk register

ID	Priority	Risk Description	Risk Category	Likelihood	Impact	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
1	Medium	Employees use shared accounts to access the system.	Access Control	3	2	2	Medium	Risk Reduction	Provide security training to target employees.	Employee D	31/12/2024	Open

After normalisation:

Departmental risk register

ID	Priority	Risk Description	Risk Category	Likelihood	Impact	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
System C ID #1, System D ID #1	Medium	Employees use shared accounts to access the system.	Access Control	3	2	2	Medium	Risk Reduction	Provide security training to target employees.	Employee C, D	31/12/2024	Open

7. Risk Monitoring and Reporting

7.1 Monitoring Identified Risks and Risk Treatment Activities

The purposes of risk monitoring may include, but not be limited, to the followings:

- Ensuring the effectiveness, efficiency, and cost-effectiveness of risk treatments.
- Gathering information to enhance future risk assessments.
- Analysing and learning from incidents, changes, trends, successes, and failures.
- Detecting changes in the internal and external context, such as risk criteria and emerging risks, may necessitate adjustments to risk treatments and priorities.

Monitoring identified risks and risk treatment activities is crucial to effective IT security risk management. Once risks are identified and recorded in the risk register, it is essential to regularly assess their status and monitor the progress of risk treatment activities. This ensures that the implemented measures can effectively mitigate the identified risks and reduce their potential impact.

The maintenance of comprehensive risk registers enables ongoing monitoring of risk activities at different levels. Risk owners should regularly assess each identified risk to determine its status, likelihood, and potential impact. The assessment can be done using expert judgment, data analysis, and historical information. Meanwhile, regularly updating the risk registers allows B/Ds to document and adapt to evolving threats and changes in the risk environment.

Furthermore, B/Ds should regularly monitor and evaluate whether the planned or implemented risk mitigation measures achieve the desired outcomes and remain relevant. This may involve gathering feedback from stakeholders, utilising performance indicators, or reassessing the impact and likelihood of the risk. Any changes or deviations from the plan should be documented and communicated appropriately. Making necessary adjustments to the treatment options based on monitoring results help ensure a proactive and adaptive approach is adopted to risk mitigation. By performing regular monitoring and assessment, B/Ds can proactively manage their IT security risks and ensure the effectiveness of their risk treatment efforts.

7.2 Monitoring the Risk Environment

B/Ds should actively monitor their risk environment for changes affecting their risk contexts. The risk environment encompasses all potential threats and vulnerabilities that could impact B/Ds' operations and objectives. Threat management is a component of the broader risk management process that focuses on identifying, assessing, and addressing threats to the B/D.

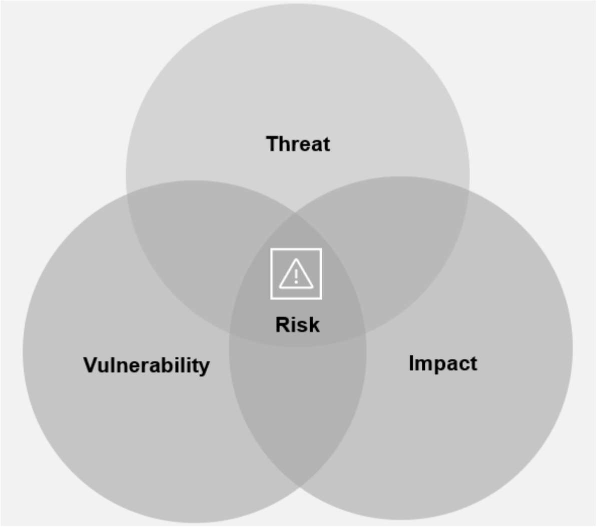

Figure 7.1 Relationship between Risk and Threat

By monitoring the risk environment, B/Ds can gain insights into emerging threats and trends, enabling them to proactively enhance their IT resilience measures and stay ahead of potential risks.

To effectively monitor the risk environment, B/Ds could employ processes such as:

- Regular vulnerability scans and penetration tests to identify and quantify security vulnerabilities.
- Utilising threat intelligence feeds to stay informed of the latest cybersecurity threats and vulnerabilities.
- Keeping track of new and existing assets through the asset management process.
- Regular reviews of user access rights to ensure they align with current roles and responsibilities.
- Regularly reviewing and updating the B/D's risk appetite statement.

Constant monitoring is essential because risk scenarios, asset values, threats, vulnerabilities, likelihoods, and impacts can change abruptly without any indication. By continually monitoring these factors, B/Ds can detect changes in the risk environment, such as:

- New sources of risk, including freshly reported security vulnerabilities.
- New assets that have been included in the risk management scope.
- Necessary modification of asset values (e.g., due to changed business requirements).
- Identified vulnerabilities to determine those becoming exposed to new or re-emerging threats.
- Changes in patterns of the use of existing or new technologies can open up new opportunities for attack.
- Changes in laws and regulations.
- Changes in risk appetite and perceptions of what is now acceptable and what is no longer acceptable.
- IT security incidents, both inside and outside of the B/D.

New sources of risk or changes in likelihood or impact can increase risks previously assessed. Hence, the risk monitoring activities should be regularly repeated, and the selected options for risk treatment should be reviewed periodically.

To monitor the trend of the risk environment, B/Ds can observe Key Risk Indicators (KRIs) and seek to determine various aspects, such as:

- Whether the likelihood of an identified risk is increasing.
- Whether the severity of the consequences is increasing.
- Whether a new risk has entered the environment.
- Whether controls are failing.

Annex C provides some examples of risk indicators for monitoring the internal risk environment.

In the event of significant changes in the risk environment, B/Ds could take the following actions:

Risk Treatment Adjustment:

- If the change represents a new type of risk, such as a zero-day attack, consider appointing a risk owner responsible for understanding the risk, developing mitigation strategies, and monitoring the risk going forward.
- Review and update risk treatment options based on the changed environment. Adjust risk treatments by directing specific actions towards particular risk scenarios to address inconsistencies or achieve different outcomes.
- This may involve tightening treatment measures to reduce the overall exposure or relaxing restrictions to gain advantages while accepting a measured increase in risk. The implementation of these changes may occur gradually to ensure comprehensive risk management at all levels of B/D.

Communication and Stakeholder Engagement:

- Communicate with relevant stakeholders about changes in the risk environment and the steps to mitigate potential impacts.
- If necessary, consider seeking external expertise advice and/or assistance to understand the change implications and help develop a strategy to mitigate potential impacts.

Modify Strategic Direction:

- Modify strategic direction by updating risk appetite statements based on collective outcomes, either increasing or decreasing risk limits. This may involve altering specific quantitative objectives and modifying the interpretation of risk tolerance to capitalise on opportunities or minimise the likelihood and impact of detrimental risks.

Monitoring and Indicators:

- Modify key performance or risk indicators to enhance visibility when the B/D changes its direction or approach to risk. Risk owners may change the Key

Performance Indicators (KPIs) and Key Risk Indicators (KRIs) being monitored. If the current indicators fail to capture changes in impact and/or likelihood adequately, it may be justifiable to introduce different or additional metrics. Increased monitoring frequency is warranted when the impact and/or likelihood of risks change more rapidly than the existing monitoring interval.

Risk stakeholders may find it helpful to develop a list of various actions to take during monitoring. For example, upon determining significant changes in particular risk areas, actions might include:

- Creating a working group to discuss and determine next steps.
- Assigning similar risk items to a centralised risk owner reduces variance and ensures accountability.
- Determining other security controls to improve protection, detection, and response in preparation for those risks that seem both likely and impactful. Such processes might include adding additional tools (e.g., logging and event orchestration), response training (e.g., incident response handling exercises), or reviewing insurance coverage.

7.3 Regular Risk Reporting

B/Ds should establish a systematic risk reporting process for risk owners to communicate risk status and treatment activities to senior management, DITSO, and other relevant parties. The risk management process and its outcomes should be documented and reported through appropriate mechanisms with the aims of:

- Communicating risk management activities and outcomes within a B/D.
- Providing information for decision-making.
- Improving risk management activities.
- Assisting interaction with stakeholders, including those responsible for risk management activities.

Regular risk reporting is essential for effective communication and decision-making within B/Ds. It is an integral part of the IT security risk management governance structure and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. Factors to consider for reporting may include, but not be limited to, the followings:

- Differing stakeholders and their specific information needs and requirements.
- Cost, frequency and timeline of reporting.
- Method of reporting.
- Relevance of information to B/D’s objectives and decision-making.

Risk reporting should include comprehensive information on the identified risks, their current status, and the progress of associated risk treatment activities. Key metrics, such as risk level, likelihood, potential impact, and KRIs, should be presented to enable stakeholders to make informed decisions. Additionally, the reporting should highlight any emerging risks or changes in the risk environment that require immediate attention or action. These reports should be prepared and circulated on a regular basis, and also when significant changes occur.

Clear and concise reporting is essential to facilitate decision-making and timely response to emerging risks. The information provided in risk reports should be easily understandable, avoiding technical jargon or unnecessary complexity. This allows stakeholders to quickly grasp the key insights and make informed decisions regarding resource allocation, risk mitigation strategies, and the overall IT security posture of the B/D.

8. Continual improvement

8.1 Feedback and Lesson Learnt

To foster a culture of continuous improvement, B/Ds should establish feedback mechanisms to capture insights and lessons learnt from past incidents, near misses, or security breaches. These mechanisms can include incident reporting systems, post-incident reviews, or regular feedback sessions with relevant stakeholders. By actively seeking feedback, B/Ds can identify areas for improvement and enhance their IT security practices. Promoting a continuous learning and improvement culture based on these experiences is vital, ensuring that B/Ds evolve and adapt to emerging IT threats effectively.

To gather feedback and derive lessons learnt in risk management activities, B/Ds can follow these steps:

(a) Collection: Establish a mechanism to collect feedback from stakeholders involved in risk management activities on the risk management framework, such as project managers, risk owners, and team members. This can be done through surveys, interviews, workshops, or regular risk review meetings.

(b) Documentation: Document the feedback and lessons learnt received from risk management activities. Include specific examples, recommendations, and actions for improvement. Disseminate this information to relevant stakeholders and incorporate it into future risk management practices.

(c) Knowledge Sharing: Encourage knowledge sharing among risk management practitioners within B/Ds. Establish protocols to share experiences, best practices, and lessons learnt across projects and departments. This fosters a culture of continuous learning and improvement in risk management.

(d) Review and Update: Regularly review and update risk management processes, procedures, and guidelines based on feedback and lessons learnt. Incorporate improvements into the IT security risk management framework to enhance future risk management activities.

8.2 Performance Measurement

Defining performance measurement metrics is crucial for assessing the effectiveness of IT security risk management within B/Ds. B/Ds should establish metrics to align with their objectives and provide measurable insights into risk management performance. Regular performance measurement and reporting are essential to track progress, identify areas for improvement, and validate control effectiveness. By analysing performance metrics, B/Ds can identify trends, benchmark against industry standards, and make informed decisions to strengthen their IT security posture.

Performance measurement in risk management involves evaluating the effectiveness and efficiency of activities and assessing the outcomes of risk mitigation efforts. It helps B/Ds understand how well they manage risks and whether their strategies and controls deliver the desired results. Key Performance Indicators (KPIs) can be defined with alignment to IT security risk management objectives. Examples include identified risks, risk mitigation effectiveness, response time, mitigation costs, and incidents or breaches.

Annex C provides some examples of performance indicators for evaluating risk treatment effectiveness.

B/Ds should regularly review and analyse performance data to identify trends, gaps, and areas for improvement. This information should be used to refine strategies, enhance mitigation activities, and strengthen the risk management framework.

8.3 Management Review and Adjustment

Regular management review of the IT security risk management activities is necessary to evaluate its effectiveness and make necessary adjustments. Senior management should regularly review the B/D's risk management process to ensure its continued suitability, adequacy, and effectiveness. These reviews should involve senior management and key stakeholders to ensure alignment with the B/D's objectives and priorities. During the review process, senior management should assess the performance of existing risk management strategies, policies, and procedures. In addition, senior management should address identified gaps or areas for improvement and make adjustments to enhance the program's overall effectiveness. Senior management involvement and support are critical to driving necessary changes and integrating IT security risk management activities into the governance framework.

Management review and adjustment aim to assure and improve the quality and effectiveness of IT security risk management activities. Review and adjustment should occur in all risk management process stages.

Below is an example of how the management review and adjustment process can be implemented in B/Ds:

Tasks	**Example of IT Security Risk Management Review and Adjustment (To be filled by B/Ds)**	**Status (Tick if completed)**
Regular management review	Conduct an annual review of the IT security risk management framework.	
Evaluate effectiveness	Evaluate the effectiveness of the current risk assessment process.	
Make necessary adjustments	Plan to adopt a new, more comprehensive risk assessment method.	
Ensure continued suitability, adequacy, and effectiveness	Review the risk management process and identify that the risk assessment process could be more comprehensive.	

Tasks	Example of IT Security Risk Management Review and Adjustment (To be filled by B/Ds)	Status (Tick if completed)
Involve senior management and key stakeholders	Involve B/D's senior management, DITSO, IT Security Management Unit, system owners and risk owners in the review process.	
Align with B/D's objectives and priorities	Decide to adopt a new risk assessment method that aligns with B/D's objectives of improving IT security.	
Drive necessary changes and integrate IT security risk management into the governance framework	Engage senior management to drive the changes in the risk management framework.	
Assure and improve the quality and effectiveness of IT security risk management activities	Monitor the results of the adjustments in the next review to ensure improved quality and effectiveness.	

*** ENDS ***

Annex A: IT Security Risk Register Template Example

ID	Priority	Risk Description	Risk Category	Impact	Likelihood	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
1												
2												
3												

- ID (Risk Identifier): A sequential numeric identifier referring to a risk in the risk register.
- Priority: A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (e.g., 1, 2, 3) or reference to a given scale (e.g., high, moderate, low).
- Risk Description: A brief explanation of the IT security risk scenario (potentially) impacting the system or B/D. Risk descriptions are often written in a cause-and-effect format, such as "if X occurs, then Y happens".
- Risk Category: Risk category groupings, such as by security and privacy control families (e.g., Access Control, Supply Chain Risk Management, such as those recorded in NIST SP 800-53). Categories could be any taxonomy that helps aggregate risk information and supports the integration of IT security risk registers for decision support.
- Impact: Analysis of this scenario's potential benefits or consequences if no additional response is provided. This may also be considered the initial assessment of the first iteration of the risk cycle.
- Likelihood: An estimation of the probability, before any risk response, that this scenario will occur. This may also be considered the initial assessment of the first iteration of the risk cycle.
- System Tier: The level of system criticality tier.
- Risk Rating: A calculation determined by the combination of impact, likelihood and other factors (e.g., system criticality).
- Risk Treatment Option: The risk treatment option for handling the identified risk.
- Risk Treatment Description: A brief description of the risk treatment. For example, "Implement software management application XYZ to ensure that software platforms and applications are inventoried" or "Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources]".
- Risk Owner: The designated individual or business unit responsible and accountable for ensuring that the risk is maintained in accordance with relevant requirements.
- Target Completion Date: The target completion date for risk treatment.
- Status: A field for tracking the current condition of the risk and any next activities. The status could be a simple indicator (e.g., open, closed, pending, waived, transferred) or provide a more detailed explanation (e.g., "risk accepted pending review by the Jan. 24 quarterly risk committee meeting"). Risk status should be a consistent set of indicators that helps aggregate risk information and supports the integration of IT security risk registers for decision support.

Annex B: Risk Category Examples for Risk Aggregation

- Asset Management
- Business Environment
- Governance
- Regulation (Compliance)
- Threat Management
- Risk Management
- Secure System Development
- Supply Chain Risk Management
- People Security
- Physical Security
- Access Control
- Data Security
- Cryptography
- Protective Technology
- IT Baseline Maintenance
- IT Event Management
- Detection Technology
- Continuous Monitoring
- Detection Process
- Incident Response & Recovery Planning
- Incident Communication
- Incident Analysis
- Incident Mitigation
- Incident Improvement

Annex C: Examples of related risk appetite, risk tolerance, controls, KPIs, and KRIs

Here are some examples of related risk appetite, risk tolerance, controls, KPIs, and KRIs:

	Example 1	Example 2	Example 3
Risk Appetite	Mission-critical systems must be protected from known cybersecurity vulnerabilities.	To safeguard protected health information, we must first ensure that only authorised parties have access to our computer systems.	Our customers associate reliability with our company's performance, so service disruptions must be minimised for any customer-facing websites.
Risk Tolerance	Systems designated as mission-critical must be patched against critical software vulnerabilities (severity score of 10) within 14 days of discovery.	We will issue unique user accounts, and our computer systems will audit positive and negative log-on events.	Regional managers may permit website outages lasting up to 2 hours for no more than 5% of its customers.
Control(s)	Periodic vulnerability assessments Patch deployment capabilities	Unique user accounts Authentication method(s) Audit logs Audit log alerting/evaluation	Power generator AC unit Upstream network provider Web load balancers Web servers
KPI	Percentage of vulnerabilities patched	Unsuccessful logins in a 1-hour period	Outage time in hours
KRI	Number of computers with critical (CVSS 10) vulnerabilities that have not been patched in 10 days	5 failed logins for a single user 30 failed logins across all users	Current outages affecting more than 5 % of customers that have lasted more than 2 hours