هـيـئـة الحكومة الرقمـيـة
Digital Government Authority

Guideline

of Risk and Business Continuity Management for Digital Government

28 January 2025
Document Type: Guideline
Document Classification: Public
Issue No. 1.0
Document Number: DGA-1-2-5-210

Contents

01. Introduction

In order to achieve the objectives of Saudi Vision 2030 and in line with the Digital Government Authority's commitment to realizing its strategic goals, as well as to enhance the reliability and continuity of digital services provided by government entities, the rapid pace of digital transformation has highlighted the need for a clear and detailed framework for risk management and business continuity within government entities. This framework ensures a comprehensive understanding of risks associated with local and global changes and their impact on the operating environment and business continuity for the digital government.

The Digital Government Authority (DGA) plays a regulatory role in digital transformation by establishing controls, standards and guidelines to enable government entities to develop the necessary capacities, methodologies and procedures to enhance their readiness in managing risks and ensuring business continuity. In this context, DGA has developed the "Guideline of Risk and Business Continuity Management for Digital Government" to elevate the maturity of risk management and business continuity practices within government entities. This initiative aims to enhance the continuity of their digital services and improve the experience of their beneficiaries.

This framework serves as a reference for government entities to support compliance with the “Controls of Risk Management and Business Continuity for Digital Government" issued by the Digital Government Authority. It further provides general guidance, not professional advice, and does not replace the requirements outlined in the local and international standards.

The application of risk management and business continuity practices depends on the specific facts and circumstances surrounding the operational environment of the government entity, related external parties, international best practices, and the regulatory requirements and standards issued by the Authority and other relevant regulatory bodies.

02. Guideline Objectives

The Guideline aims to support government entities to comply with the risk management and business continuity controls for digital government issued by the Digital Government Authority, and achieve the following objectives:

1. Enhancing integration among government entities and strengthening the resilience and flexibility of digital government services to ensure digital services continuity while reducing costs during incidents and crises.

2. Promoting risk management and business continuity practices within government entities in alignment with best standards, through the implementation of effective and clear methodologies and identification of tools to improve the efficiency and effectiveness of procedures.

3. Cultivating a culture of risk management and advancing maturity, including fostering a culture of business continuity management and compliance with regulatory requirements to improve the digital government services delivered to beneficiaries.

4. Ensuring business sustainability and protecting the reputation of government entities by adopting a proactive approach to risk management, identifying appropriate mitigation strategies, and optimizing the use of resources and capabilities to protect and enhance the reputation of the digital government.

03. Guideline Scope

This Guideline includes the most important instructions for designing and implementing the framework and basic components of the risk management and business continuity management systems in line with the operations of the government entity. The Guideline includes:

A. Risk Management System Instructions This section explains the components of the risk management system, its importance and its principles, with examples of the most prominent relevant international and local standards. It also details the stages of the risk management system methodology and guidance.

B. Business Continuity System Instructions This section explains the importance of the business continuity management system, and the most important benefits resulting from its implementation, followed by its principles and success factors, in addition to examples of the most prominent local and international standards. It also details the stages of the business continuity management system methodology and guidance.

C. Documents Management: This section explains the instructions for keeping data, documents and forms for the risk management and business continuity management systems, and automation of the two systems.

04. Targeted Audience

Government entities that provide digital services and products, as well as operators and relevant stakeholders, regardless of their type, size, or nature of operations The applicability of the instructions and recommendations depends on the operational environment of the government entity, the scale of its operations, and its geographical locations.

05. Statement of the Guideline

- 5.1 Risk Management System
- 5.2 Business Continuity Management System

5.1

Risk Management System

5.1 Risk Management System

A Risk Management System is defined as a structured and integrated approach led by senior management and decision-makers within a government entity. It encompasses a set of strategies, policies and procedures aimed at mitigating emerging and existing risks, as well as managing residual risks that the entity may face, and could hinder the realization of its strategic and operational objectives. This system involves the application of methodologies, tools and processes to anticipate, identify, analyze and evaluate and prioritize risks, and continuously monitor and review them. It also includes preventive measures and strategies to minimize the likelihood of their occurrence and mitigate their negative impacts, as illustrated in Figure (1).

Figure (1): Risk Management System

5.1.1 Importance of Risk Management System

The importance of risk management lies in supporting and enhancing strategic and operational decision-making by senior management, committees and stakeholders in the government entity. It also contributes to effectively achieve the objectives of the government entity to mitigate the possibility of risks and their impact, and reach an acceptable level of risk for the government entity. Figure (2) below illustrates the main benefits and gains of implementing a risk management system in the government entity, as per the following details:

Figure (2): Most Important Benefits of Risk Management System

- **Proactive and Decision-Making Support**

Enabling the government entity to proactively identify potential risks and support strategic and operational decision-making by stakeholders.

- **Improving Efficiency & Effectiveness**

Applying and implementing an effective framework for the Risk Management System that leads to improving the efficiency and operational effectiveness of the government entity, and optimizing the use of resources and capabilities.

- Promoting a Culture of Risk Awareness

Promote a culture of risk awareness and adopt a risk management-based approach to identify potential risks and develop appropriate treatment strategies and plans to address them proactively and avoid negative impacts.

- **Enhancing Business Resilience and Sustainability**

The ability to enhance the business continuity processes and plans within the government entity by supporting the processes of assessing risks and internal and external threats that affect the government entity's business.

- Supporting the Realization of Strategic Objectives

Identifying opportunities and threats that may affect the realization of the strategic objectives of the government entity, and developing plans and initiatives to address and deal with them.

5.1.2 principles of Risk Management System

The international standard for risk management, ISO 31000:2018, issued by the International Organization for Standardization, is based on eight (8) fundamental principles for a risk management system, as outlined in Table (1). These principles are designed to be implemented within government entities to achieve advanced maturity levels and effective risk management processes:

#	Principle	Description
1	Integrated	Including and considering risk management as an essential part of all government entity's operations and activities, and supporting proactive decision-making.
2	Structured and Integrated	Following a systematic and comprehensive approach to the risk management system and processes, in cooperation with stakeholders in the government entity. This approach leads to clear, comparable and measurable results.
3	Dedicated	Implementing a risk management system commensurate with the internal and external context and scope of the government entity's operations, in a manner that ensures a close link with its strategic objectives.
4	Comprehensive	Enabling the participation of stakeholders in appropriate situations and times, and taking into account their views and experiences. This leads to raising awareness and increasing the effectiveness of the risk management system.
5	Dynamic	Anticipating risks resulting from changes in the internal and external context and scope of the government entity, as well as changes in strategic objectives and directions, and dealing with them in an appropriate and timely manner.
6	Information-Driven	Ensuring that the Risk Management Unit is consistently provided with accurate, complete, and timely information by stakeholders and relevant parties, without any restrictions on access permissions to this information. The inputs of the risk management system rely on past, current, and emerging information, as well as future projections based on these inputs.
7	Humanitarian and Culturally Sensitive	Taking into consideration the significant impact of human behavior and the cultural levels of government entity staff on all aspects and stages of the risk management system..
8	Supportive of Continuous Improvement.	Continuously improve and develop the processes and activities of the Risk Management System through previous events, knowledge and experiences built on the effective application of the risk management system, as well as the training sessions and workshops provided. This aligns with the evolving scope and operations of the government entity.

Table (1): Principles of the Risk Management System

5.1.3 Risk Management System Success Factors

The successful implementation of the mechanisms and procedures of the risk management system of the government entity depends on a set of success factors, most prominently:

Integration of Risk Management into Decision-Making Processes:

- Including risk management as a key component in the decision-making process.
- Support and interest of leaders and senior management in implementing the requirements of the Risk Management System.

Transparency, Independence and Understanding of Risks:

- Supporting transparency and providing the best inputs from various sources to understand and assess both internal and external risks of the government entity.
- Applying the risk management system methodology in an organized manner contributes to raising efficiency levels and ensures accurate, reliable, transparent and objective results.
- Automating processes related to the risk management system ensures the effectiveness of the risk methodology and the accurate and continuous issuance of reports.

Empowering the Risk Management System

- Ensuring the independence and empowerment of the unit responsible for the risk management system, thus improving the government entity's performance.
- Designing the risk management methodology to align with the internal and external context of the government entity.

Monitoring the Risk Management System

- Monitoring the effectiveness of risk management system’s tasks and activities, and adhering to and applying international standards and practices, and local regulations.

5.1.4 Risk Management System Standards

There are many local and international standards and regulations for the risk management system, as well as frameworks, principles and guidelines that support the construction and activation of the risk management system. It also contributes to the identification of risks, the promotion of plans to address risks and exploit opportunities through the application of best practices with high efficiency. Among the key local standards used to establish and activate the risk management system are the Risk Management and Business Continuity Controls for Digital Government issued by the Digital Government Authority, and the Frameworks and Guidelines issued by the General Secretariat of the National Risk Council. Regarding international standards, some of the most prominent include: The ISO 31000:2018 Risk Management Standard issued by the International Organization for Standardization (ISO). The COSO Enterprise Risk Management Framework 2017. The Australian/New Zealand Risk Management Standard (AS/NZS 4360).

The Risk Management Standard by the Institute of Risk Management (IRM). Additionally, many countries have issued risk management guidelines, including: The Orange Book – Principles and Concepts of Risk Management, issued by the UK government. The Risk Management Guide for the Public Sector, issued by the Government of British Columbia in Canada. The Risk Management Guide issued by the Independent Verification and Validation Program at NASA.

5.1.5 Risk Management System Methodology

The methodology for building and operating the risk management system aims to raise the readiness level of the government entities, and enhance the treatment of risks, as mentioned in the Risk Management and Business Continuity Controls for the Digital Government issued by the Digital Government Authority. Figure (6) and Figure (3) show the stages of the methodology, as follows: Building and governance of the risk management system, activating risk management processes, training and improvement of the system.

Figure (3): Building and Governance of the Risk Management System

5.1.5.1 Building and Governance of the Risk Management System

This phase outlines how to build and design the key components for activating risk management within the government entity. The aim is to establish a policy, framework and procedures for risk management that align with the government entity's needs, and thereby supporting senior management in achieving its strategic objectives (Figure 3).

5.1.5.1.1 Building and Governance Risk Management System Policy

The risk management policy is the primary driver for managing the system and creating and developing the components of the risk management system, including roles and responsibilities, procedures, processes and methodologies.

- Components of the Risk Management Policy

The risk management policy consists of a set of essential elements, including at least the following Introduction and definition of the policy, objectives of the policy, scope of application, organizational and administrative structure of the risk management system, general controls of the policy, roles and responsibilities, matrix of powers for relevant internal and external parties, mechanism for periodic review of the policy, as well as approval by the competent authority in the government entity. Figure (4): Key Elements of the Risk Management Policy

Figure (4): Key Elements of the Risk Management Policy

- Introduction and Definition of the Risk Management Policy

The introduction and definition of the risk management policy, reference frameworks and standards, and the core values and principles guiding the risk management process within the government entity are developed and clarified. This enables the government entity to handle potential risks it may face due to economic social, and political changes, in order to achieve its strategic and operational objectives effectively and efficiently.

- Objectives of the Policy

The objectives of the risk management policy of the government entity are defined and stated to achieve tangible results and benefits from its implementation. These objectives include enhancing the ability to predict risks and manage them effectively, improving the overall performance of the entity, and increasing its resilience in facing both internal and external challenges.

- Scope of the Policy

The scope of applying the risk management policy is developed and documented, including: the relevant administrative units, stakeholders and service providers. It covers activities and processes related to risks, to ensures effective coordination between all involved parties.

- Organizational and Administrative Structure of the Risk Management System

The organizational and administrative structure of the risk management system is clarified, including: the relevant committees and the administrative units responsible for the risk management system. This point is further detailed in section (5.1.5.1.1), which includes models of the organizational and administrative structure for the risk management system, where the structure defines the relationships between the parties involved in risk management.

- General Controls of the Policy

The general controls of the risk management policy are developed and stated, including the main rules and basic standards that must be considered when implementing the risk management policy, the processes applied, and the tools used for managing the risks within the government entity. These controls aim to ensure the effectiveness of risk management and the achievement of its objectives

- Roles and responsibilities, matrix of powers for relevant internal and external parties

The different roles and responsibilities of stakeholders and all those involved in the risk management system are clarified and mentioned, starting from the Board of Directors, through the employees of the government entity and external parties, such as contractors, suppliers and partners. Section (5.1.5.1.1) gives an illustrative example of the roles and responsibilities of the risk management system.

- Mechanism for Periodic Review of the Policy

A mechanism for the periodic review of the risk management policy is established and clarified, in align with the internal and external work environment, the changes faced by the government entity, and the relevant legislative and regulatory requirements.

- Approval by the Competent Authority in the Government Entity

The approval of the risk management policy by the competent authority at the government entity is documented upon the creation of the policy, as well as during periodic updates, to enhance compliance with the policy by all personnel of the government entity.

- **Governance of the Risk Management System**

Risk management governance is a key component of building an effective and consistent framework for managing risk business and activities at the government entity level, where the roles and responsibilities of all parties involved in the risk management system are clarified, and the structure is clarified and closely linked to the supervisory committees, senior management, and both internal and external stakeholders.

- Building the Administrative Unit Responsible for the Risk Management System and Related Committees

A manager is appointed for the administrative unit responsible for the risk management system, along with forming and selecting team members and equipping them with the necessary skills to establish and develop the system. It is crucial that team members understand the unit's responsibilities and objectives. Additionally, the required resources for implementation processes are provided, alongside support and assistance to achieve the strategic goals of the unit.

- The Three Lines Model for Risk Management

The Three Lines Model for Risk Governance (Figure 5), previously known as the Three Lines of Defense Model, issued by the Institute of Internal Auditors, explains the collaborative relationship among the various administrative units within the government entity to address risks. The significance of this model lies in fostering cooperation and interconnectedness across all executive, administrative and operational levels of the government entity to manage surrounding risks and threats effectively.

- First Line/ Level: Represents all operational activities.
- Second Line/ Level: Represents the administrative units responsible for governance, compliance, risk, and cybersecurity, to ensure compliance with the policies, standards and procedures approved by the government entity.
- Third Line/ Level: Represents the administrative unit responsible for internal audit/ review, and the independent unit responsible for verifying the maturity level of the risk management system processes. This Line highlights and presents the risks and controls to senior management or the Board and Committees within the government entity.
- In addition to the above, external auditing and review play a critical role in providing assurance to stakeholders regarding compliance with relevant legislation and regulations.

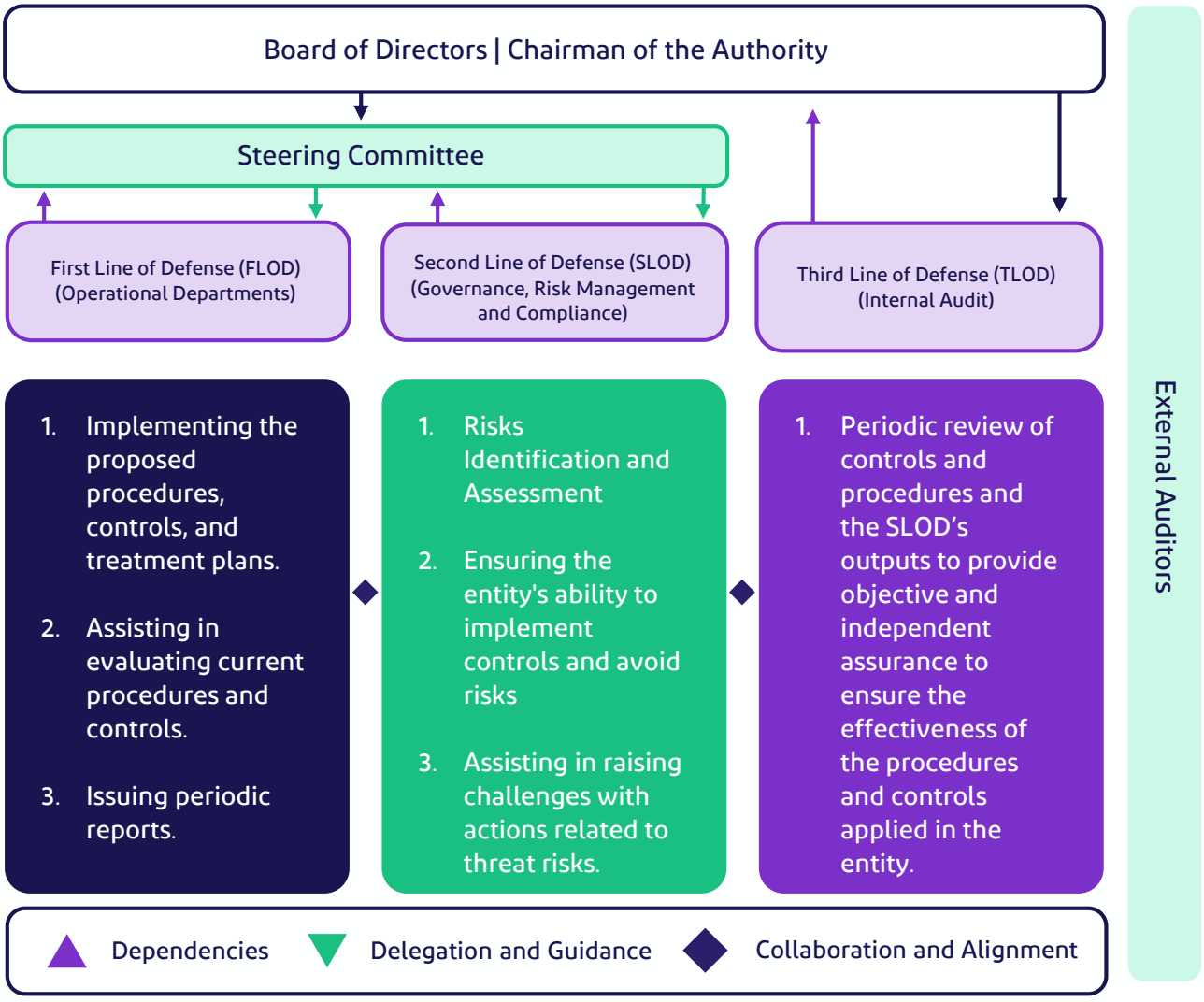


Figure (5): Three Lines Model

- Organizational Structure of the Risk Management System – in Case There is a Board of Directors for the Government Entity
  (Form 1):

Figure (6) shows a model of the organizational structure in the case there is a board of directors for the entity. It includes the risk committee emanating from the board of directors, the steering committee, and the administrative unit responsible for the risk management system.

Figure (6): Illustrative Example of Form 1 - Organizational Structure of Risk Management System

- Organizational Structure of the Risk Management System – in the Absence of a Board of Directors for the Government Entity (Form 2):

(Figure 7) shows a model of the organizational structure in the absence of a board of directors for the entity.

It includes the steering committee and the administrative unit responsible for the risk management system.

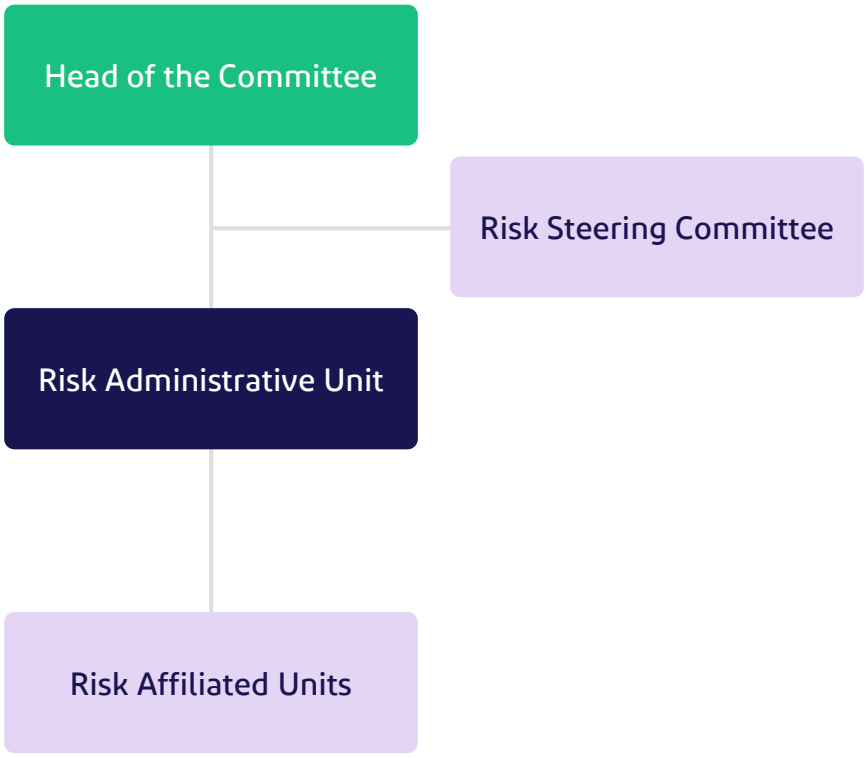


Figure (7): Illustrative Example of Form 2 - Organizational Structure of Risk Management System

- Roles and Responsibilities of the Risk Management System

Defining the roles and responsibilities of the risk management system contributes to enhancing transparency and accountability, raising efficiency and effectiveness in business performance, and applying risk management practices. This section clarifies the most important roles and responsibilities of the parties related to the risk management system[1]:

[1]The above roles and responsibilities are only indicative examples, and the roles and responsibilities vary from one side to the other depending on the nature of the business.

1. Board of Directors[2]:

- Supervising the risk management system and fostering a risk culture within the government entity.
- Ensuring, supporting and guiding the independence of the administrative unit responsible for the risk management system, in accordance with the organizational structure of the government entity. Additionally, ensuring the availability of sufficient financial and human resources to support the implementation and execution of risk management operations.
- Guaranteeing clarity of roles and responsibilities related to the risk management system to support effective governance and enhance decision-making across all executive, administrative and operational levels.
- Approving the risk management strategy, policy, framework, and appetite and tolerable risk levels.
- Overseeing the integration of risk assessments and acceptable and tolerable risk levels into strategic decision-making processes

2. The Chief Executive in the Government Entity:

- Approving methodologies, risk indicators, risk governance models, the roles, responsibilities and authority matrix, as well as performance measurement indicators for the risk management system within the government entity.
- Providing overall supervision of the implementation of the risk management system across all administrative units and operations within the government entity.
- Forming the internal steering committee responsible for the risk management system

3. Risk Committee emanating from the Board of Directors (if any)[3]:

- Verifying the effectiveness of identifying and assessing Key risks and implementing mitigation plans, including oversight actions taken by the government entity to manage risks.

[2]If the government entity does not have a Board of Directors, the authority is delegated to the Chief Executive of the entity.

[3]If the government entity does not have a Risk Committee emanated from the Board of Directors, the authority is delegated to the Risk Steering Committee.

- Reviewing the Key risk report periodically or as needed, particularly in the event of significant changes within the government entity.
- Reviewing and assessing the actions taken by the government entity to monitor and manage exposure to all types of risks.
- Reviewing and recommending the approval of the risk management strategy, policy, framework, and risk appetite and tolerance document before submission for approval by the Board of Directors.
- Reviewing annual reports from internal and external auditors on the implementation of the risk management system's policies and procedures within the government entity, and providing recommendations and support for system improvements, as needed.
- Reviewing and approving high and critical risks, as well as key risk indicators in specified cases, while providing support for necessary actions and implementing mitigation plans.

4. Risk Steering Committee:

- Ensuring compliance with the approved Risk Appetite and Tolerance Document and escalating any breaches to senior management, the Board of Directors, or the Risk Management Committee emanated from the Board, as deemed necessary by the committee, and providing recommendations regarding such breaches.
- Regularly following up on the procedures for identifying, analyzing and assessing risks.
- Monitoring and tracking the implementation status of the entity's mitigation plans for major and critical risks.
- Guiding administrative units within the government entity to provide the necessary support for implementing risk assessment procedures and practices.
- Periodically reviewing risk management reports to analyze the overall risk status.
- Providing support and supervising the effectiveness of training programs, awareness initiatives, and specific risk management programs within the government entity.
- Regularly monitoring and tracking key risk indicators.
- Controlling and monitoring the maturity level of the risk management system practices to ensure that the best standards and practices are applied.

5. Administrative Unit responsible for the Risk Management System:

- Preparing, developing and updating the risk management's strategy, policy, framework and procedures, and ensuring that the administrative units within the government entity comply with the risk management policy and procedures.
- Preparing and developing the methodology for risk management processes within the government entity, including: Risk assessment methodology and risk self-assessment process. Supervising the effective implementation of the methodology.
- Preparing programs, plans, methodologies, guidelines, indicators, governance models, matrices of roles, responsibilities, and authorities, and performance measurement indicators specific to the risk management system. These are developed in coordination with the relevant departments of the government entity, submitted to the Chief Executive for approval, implemented following endorsement, monitored, adhered to, reviewed, and updated.
- Creating and updating all risk registers for the administrative units within the government entity and identifying key risks in collaboration with the risk owners. Additionally, developing mitigation plans with risk owners to reduce risks and reporting them according to the approved risk management framework.
- Establishing and updating key risk indicators (KRIs) as well as key performance indicators (KPIs) and submitting periodic reports to the steering committee and stakeholders.
- Monitoring risks, threats, and internal and external factors that may negatively impact the performance of the government entity, and submitting related reports to the risk steering committee and stakeholders on a regular basis.
- Preparing reports on key risks within the government entity and submitting them periodically to the risk steering committee and stakeholders.
- Ensuring an annual risk assessment for the entire government entity
- Coordinating and organizing training programs and workshops related to the risk management system to enhance risk awareness among all employees of the government entity.

6. Risk Owners

- Identifying, analyzing and evaluating existing and emerging risks, and reporting them in coordination with the administrative unit responsible for the risk management system in the government entity.

- Managing existing risks within their responsibilities on an ongoing basis, and participating in workshops to identify and assess risks.
- Developing corrective actions, treatment plans for identified risks, and monitoring their timely implementation.
- Reporting periodically, or upon request, on the status of risks to the administrative unit responsible for risk management.

7. Owners of Treatment Plans

- Aligning with the risk owner and the administrative unit responsible for the risk management system to determine the appropriate risk treatment strategy and define the detailed plans.
- Implementing treatment plans and submitting implementation progress reports to the administrative unit responsible for the risk management system on an ongoing basis.

8. Risk Champions

Risk Champions are considered one of the key components of the system. A representative is nominated from each administrative unit within the government entity based on their respective areas of expertise. They provide support in activities aimed at fostering risk awareness within their respective business units and departments. Additionally, they serve as points of contact for identifying and analyzing relevant risks. Risk Champions work closely with risk owners to identify any changes or emerging risks and report them to the administrative unit responsible for the risk management system. They monitor risks, assess their impact, and make recommendations of corrective actions to the administrative unit responsible for managing risks.

9. Internal Auditing

- Providing assurances to stakeholders of the effectiveness of risk management procedures, and ensuring that the effectiveness of internal controls is assessed in proportion to the risks appropriately identified.
- Reviewing risk management policy and procedure evaluations.
- Evaluating the models and procedures of the risk management system.
- Reviewing the risk management system processes, and making recommendations to stakeholders that will develop and improve the effectiveness of the risk management system.

10. Departments or Units related to Risk Management Processes

- Aligning with the risk management framework and methodologies in relevant risk assessments.
- Providing the administrative unit responsible for the risk management system with risks-related information and reports.

11. Government Entity's Employees

- Reviewing documents related to the risk management system, such as: Risk Management Policy, Risk Management Framework, and Risk Procedures.
- Identifying the relevant risks and reporting them to the administrative unit responsible for risk management, emphasizing that risk management is a collective responsibility. Additionally, coordinating with the unit regarding the risk management system and providing the required documents upon request.
- Attending all awareness sessions, workshops, and/or training courses related to the risk management system.

- Skills required for the Work Team

Qualified human resources form one of the key pillars for the effective implementation of the risk management system. The recruitment of competent individuals with the appropriate qualifications and experience enhances the capabilities of the risk management system and supports the efficient execution of risk management practices and activities. Professional certifications and specialized qualifications in the field of risk management play a crucial role in improving and elevating knowledge, and improving skills and experiences, thereby contributing to enhanced performance at both the individual and government entity levels.

The most important professional certificates specialized in the risk management and business continuity system are mentioned in (Appendix 12.2), and they are classified based on experience and job level. The most important technical skills required for the risk management team are shown in (Table 2) below.

#	Description
Communication Skills	
1	The ability to present and communicate various information, such as conveying ideas and accepting different perspectives, while considering the diversity and differences among the government entity's employees.
2	The ability to enhance internal and external communication with stakeholders and relevant parties to solve problems or progress in achieving goals.
Teamwork Skills	
3	The ability to strengthen partnerships with the various administrative units in the government entity in order to identify and implement initiatives and activities, and support the participation of the government entity's employees in the risk management system.
4	The ability to deal with challenges constructively, and work with other parties to find appropriate solutions.
Strategic Thinking Skills	
5	The ability to analyze and use data to make appropriate long-term decisions.
6	The ability to envision the future based on evidence and facts, prioritize tasks, break down complex problems, think outside the box to find effective solutions, and implement actions in alignment with the analyzed data.
Technical Skills	
7	The ability to use appropriate tools and techniques for the risk management system in accordance with best practices and standards.
8	The ability to collect data and information from its correct sources, and examine, analyze and verify its accuracy for the purpose of inferring information that helps to make appropriate decisions.
9	The ability to use evidence-based knowledge and scientific evidence to enhance accumulated experience and acquired skills with the aim of continuous development and improvement.
10	Thinking logically and analytically about risks, estimating the impact and likelihood of expected risks, and dealing with them in a professional manner.
Leadership Skills	
11	The ability to make effective and efficient decisions, aligning available information and methods to achieve desired objectives, while considering laws and potential impacts when making decisions and taking responsibility for them.
12	The ability to create a positive environment, direct others' thinking towards a specific goal, and work to create a practical and collaborative shared vision with stakeholders.
13	The ability to negotiate with others and reach appropriate solutions for all parties, and the ability to develop ways and methods of negotiation.

Table (2): The Most Important Skills required for the Risk Management Team.

- Governance of Risk Committees

Internal and external risk committees oversee the integrated leadership, administrative and operational roles related to risks within the government entity.. Committees are formed and approved to follow up risks at the level of leaders within the government entity, and they are subject to the supervision of the senior management or the board of directors in the government entity and chief officer. These committees submit periodic reports on risks and take the necessary measures effectively, in order to ensure the implementation of its main tasks. Figure (8) illustrates the communication mechanism for risk committees and the supervisory role in monitoring the effectiveness of the risk management system within the government entity:

- The strategic direction and the entity's risk appetite are determined by the Board of Directors.
- Risk committees regularly follow up on risk reports and the effectiveness of the risk management system according to the recommendations of the Board of Directors and the steering committee.
- The administrative unit responsible for the risk management system implements the system, identifies, analyzes, and evaluates risks in collaboration with relevant departments, and submits reports to the risk committees.
- The internal audit department monitors the performance indicators of the risk management system by requesting reports from the relevant departments and periodically submitting them to the risk committees*.

*The risk committees consist of the risk committee emanated from the board of directors and the risk steering committee.

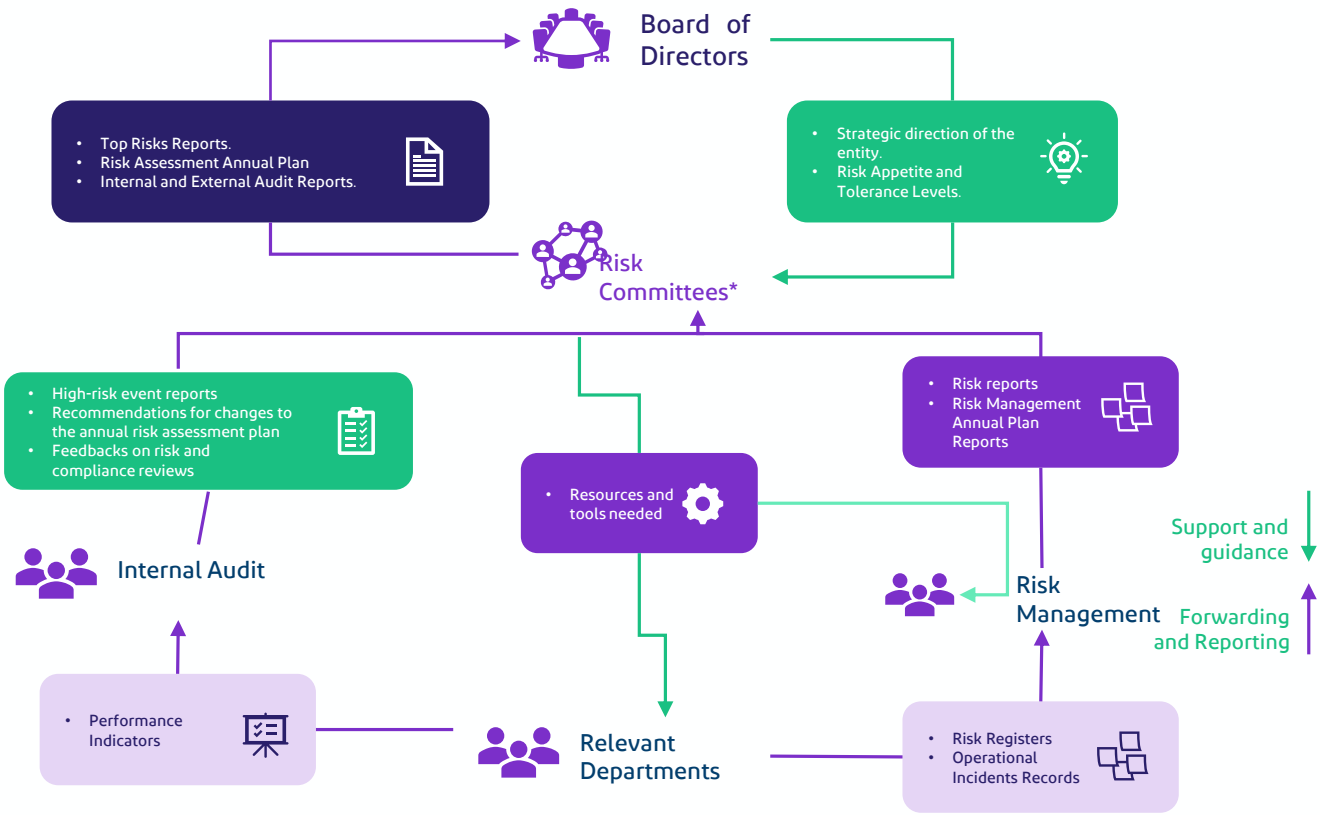


Figure (8): Illustrative example of communication between Risk Monitoring Committees

5.1.5.1.2 Developing Risk Management Strategy

The risk management strategy defines the risk management objectives by building a document compatible with the objectives and strategies of the government entity, aligning it with the Saudi Vision 2030. A key factor in realizing the risk management's objectives and strategy is to periodically assess the maturity level of the risk management system to ensure that the realization of the strategic objectives of the entity. The maturity level of the risk management system is measured based on a set of elements. For example, Figure (9) below shows a number of key elements to assess the level of maturity:

Figure (9): Elements of Assessing the Risk Management Maturity Level

- **Components of the Risk Management strategy**

The strategy document helps unify and guide risk management efforts, and improve performance, efficiency and effectiveness. The document includes a set of elements, the most important of which is shown in Figure (10).

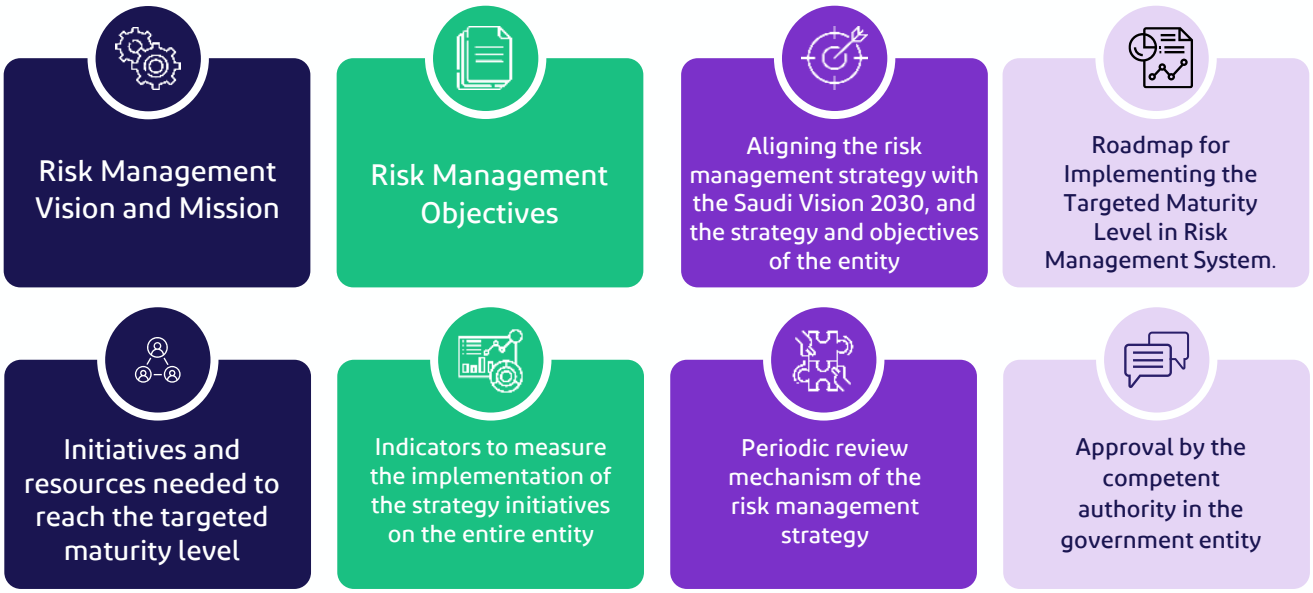


Figure (10): Most Important Items of the Risk Management System

- Risk Management Vision and Mission

The vision and mission of risk management in the government entity are defined, developed and drafted to reflect the strategic direction and long-term objectives related to the risk management system, in alignment with the entity's vision and mission. The vision represents the desired goal for the risk management system, aiming to achieve the highest standards of effectiveness and efficiency in addressing challenges and potential risks. The mission is similarly defined and drafted to clarify the foundational principles that guide the activities and initiatives in this area, including a commitment to integrity, excellence and innovation, as well as internal and external collaboration within the entity in the field of risk.

- Risk Management Objectives

The objectives for establishing the risk management system, emanated from the vision and mission of risk management, are clearly defined and measurable. Internal and external objectives are coordinated and directed to ensure alignment with the entity's strategic directions.

- Aligning the Risk Management Strategy with the Saudi Vision 2030 and the Government Entity's Objectives

The alignment between the strategic objectives of the risk management system and the strategy and goals of the government entity, as well as with Saudi Vision 2030, is clarified. This process reflects the entity's comprehensive vision towards sustainable development and success, where it achieves harmony between the goals of the risk management system and the entity's objectives.

- Roadmap for Implementing the Targeted Maturity Level Assessment in the Risk Management System

The maturity level of the current risk management system of the entity is evaluated and identified, and an operational plan is developed to identify activities to reach a high level of maturity within a specified period of time. This aims to ensure the implementation of the risk management system efficiently and effectively, and to achieve the strategic objectives of the entity.

- Initiatives and Resources needed to reach the Targeted Maturity Level

Plans, initiatives, operational projects, activities, and the necessary human, financial, and technical resources for implementing the roadmap and achieving the targeted maturity level are determined and developed, taking into account the internal work environment, regulatory requirements, and the directions of senior management and stakeholders.

- Indicators for measuring the implementation of strategic initiatives across the entire government entity.

Performance indicators are defined and developed to measure the effectiveness of implementing the initiatives and projects related to the risk management system. Progress in executing these initiatives and projects is evaluated, determining the extent to which these initiatives achieve the desired deliverables and their impact on the government entity to ensure that the strategic objectives of the risk management system within the government entity are achieved.

- Periodic review mechanism of the risk management strategy

A mechanism is developed for the periodic review of the risk management strategy to ensure the efficiency of the objectives and the effectiveness of achieving the roadmap, in line with the internal and external business requirements and regulatory requirements. It also reviews the changes that the government entity may experience during the implementation of the roadmap to achieve the objectives of the risk management system.

- Approval by the Competent Authority in the Government Entity

The approval of the risk management strategy by the authorized person in the government entity is documented both when the strategy is initially created and during regular updates, to support the implementation of the strategy.

5.1.5.1.3 Developing Risk Management Framework and Procedures

The risk management framework is developed and created, including the methodology, mechanisms, and procedures necessary to implement risk management operations and activities. This includes clarifying the methodology for identifying, analyzing, and assessing risks, as well as specifying and developing appropriate risk mitigation strategies tailored to the nature of the government entity's operations. To effectively develop a risk management framework, the following must be comprehensively understood and assessed:

- Understanding and evaluating the national trends, Vision 2030, and the digital transformation strategies.
- A complete and accurate understanding of the government entity's strategies and objectives.
- Understanding the government entity’s strategic and operational performance indicators.

As shown in Figure (11), the framework includes essential elements that contribute to building an effective risk management framework.

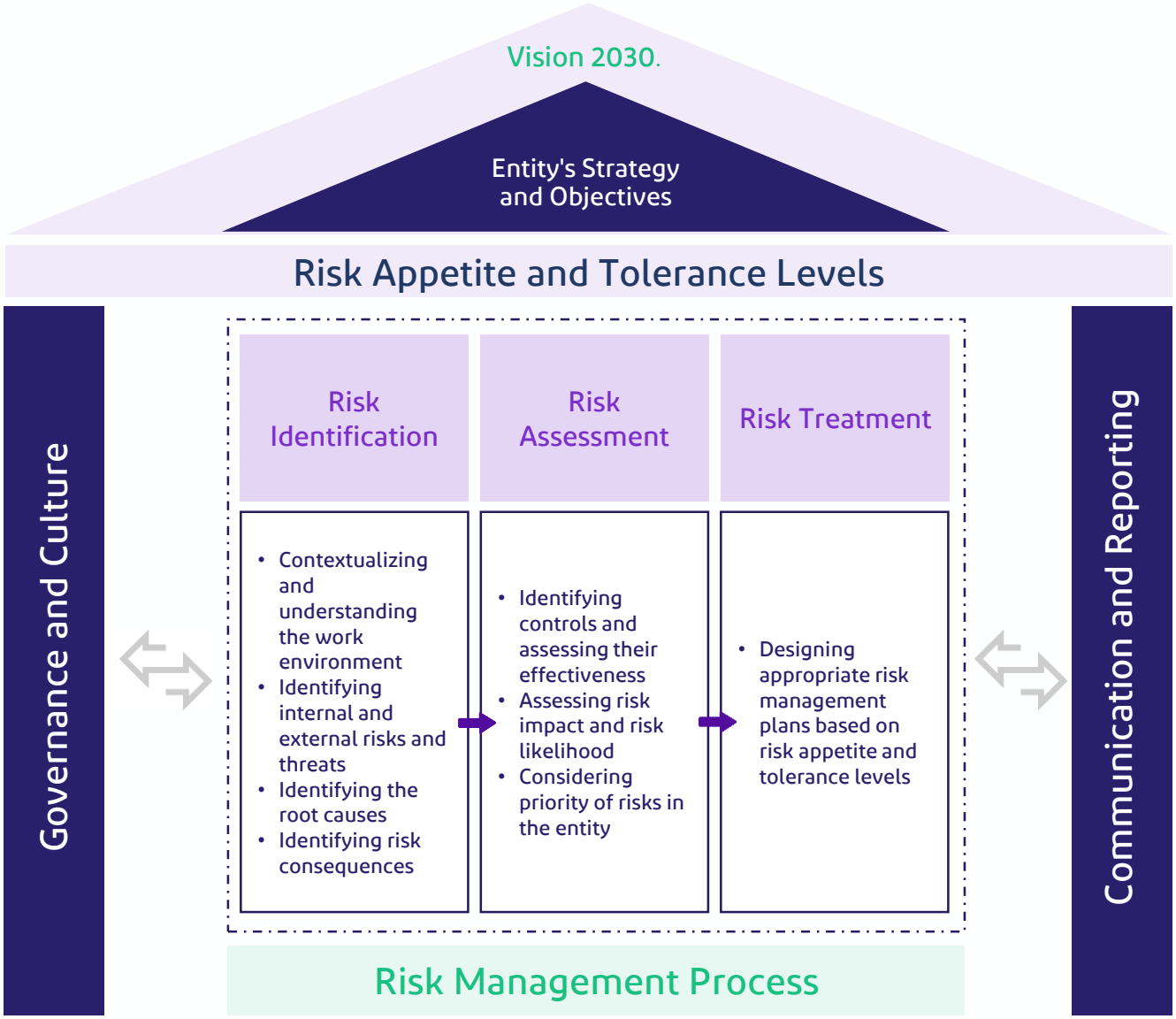


Figure (11): Risk Management Framework

- Components of the Risk Management Framework

The creation of a risk management framework aims to improve decision-making, allocate resources, ensure compliance with regulations and standards, enhance resilience in risk management operations, and enable flexible planning. Figure (12) illustrates the key components of the risk management framework.

Figure (12): Most Prominent Items of the Risk Management Framework

- **Context, scope, and objectives of the risk management framework and linking them with the objectives of the government entity**

The internal and external context of the risk management system is defined and built, including all internal and external factors and business requirements that affect the performance of the risk management system and the scope of work. This aims to ensure the quality of the risk management system, and it covers all aspects and activities associated with the government entity. In addition, identifying the main objectives of the framework in line with the vision and strategic objectives of the entity.

- **Risk Management Methodology**

The risk management system methodology is mentioned to clarify the ways, methods and tools used to implement risk management activities, taking into account that they align with the services and products provided by the government entity to the beneficiaries, and consistent with the objectives, nature and volume of the business within the government entity, as well as the internal and external risks that it may encounter.

- **Identifying Categories of Main Risks in the Government Entity**

Risk categories are defined to include different classifications of internal and external risks that the government entity may encounter. Risks are classified to main risks and sub-risks, and the nature and categories of risks that the government entity may face vary according to the internal and external work environment, and the size of the business it carries out.

- **Determining Likelihood and Impact levels, as well as Risk Assessment Matrix**

A probability matrix is defined to determine the likelihood levels of risk occurrence. An impact matrix is defined to determine the levels of impact resulting from the risks, and a risk assessment matrix is defined to determine the severity level of the identified risks.

- **Mechanism for Identifying, Analyzing and Evaluating Inherent and Residual Risks in the Government Entity**

The foundations are developed and established to define the steps, procedures and tools used to identify, analyze and assess both inherent and residual risks within the government entity. These foundations are clear, actionable and aligned with the operational processes of the entity and the internal and external risks it faces.

- **Identifying Types of Controls and the Mechanism to Assessing their Effectiveness**

The types and categories of controls, mechanisms and tools used to evaluate the effectiveness of the design and operation of those controls are clarified by the government entity, aiming to ensure the effectiveness of the controls applied to reduce the impact of risks and unsustainability of the government entity's business.

- **Determining the Methodology for Selecting Risk Treatment Strategies**

The methodology for selecting risk treatment strategies shall be determined and clarified based on the risk appetite and tolerance levels adopted by the government entity, and the directions and views of stakeholders to ensure that the objectives of the government entity are achieved with the lowest possible risks.

- **The Mechanism for Implementing Treatment Plans, including the Maximum Periods for Implementation and Risk Assessment Results**

The steps followed to implement and apply the treatment plans in the government entity are clarified, including identifying the owners of the treatment plans. These steps shall clearly define the responsibilities and specify the expected timelines to follow up the implementation of the plans efficiently and on time.

- **Mechanism and Criteria for Identifying Key or Principle Risks in the Government Entity**

The steps and criteria followed to identify the Key or Principle risks in the government entity are identified, based on specialized methodologies to ensure accurate and comprehensive risk analysis. These steps enhance the ability to identify key risks that represent a major threat to the objectives of the government entity.

- **Mechanism for Defining Key Risks Indicators (KRIs)**

The steps and tools used to identify key risk indicators are identified and clarified. Further, the monitoring mechanism and the periodicity of review and follow-up by those concerned in the government entity are also clarified, thereby contributing significantly to improve the ability to identify and address potential risks effectively and quickly.

- **Mechanism for Reviewing and Monitoring Risks of all Types and Levels in the Government Entity**

The steps and tools used to review and monitor all risks are identified and clarified by the administrative unit responsible for the risk management system, including the review frequency. This helps to identify any changes in the internal and external environment of the entity, as well as the mechanism for submitting recommendations and procedures needed to effectively address risks.

- **Mechanism of Communication and Submitting Advices regarding Risks in the Government Entity, both Internally or Externally**

The steps and tools used to communicate, receive and advise on risks are defined to ensure the effective exchange of information and guidance among stakeholders and relevant parties.

- **Risk Reporting Mechanism for Stakeholders and Relevant Committees both inside and outside the Government Entity**

The steps followed for reporting risks are determined, including the types of reports, and reporting frequency based on the type and importance of risks, as well as the committees and stakeholders in the government entity.

- **Risk Escalation Mechanisms**

The steps and methodology followed to escalate risks, the time frames for each stage of escalation, and the roles and responsibilities of those concerned inside and outside the government entity are identified and mentioned.

- **Periodic Review Mechanism of Risk Management Framework**

A mechanism for the periodic review of the risk management policy is established and clarified, in alignment with the internal and external work environment, the changes faced by the government entity, and the relevant legislative and regulatory ، requirements.

- **Approval by the Authority in the Government Entity**

The approval of the risk management framework by the authorized person in the government entity is documented both when the framework is initially created and during regular updates, to support the implementation of the framework by the relevant parties.

- Risk Management System Procedures

Risk management procedures provide the government entity with the appropriate mechanisms to implement risk management activities. Risk management procedures are an essential part of effective governance and contribute directly to enhancing the ability of the government entity to achieve its objectives.

These procedures begin with the identification of risks, where the risk management team analyzes the various scenarios that the government entity may face, and identifies factors that may pose a threat to its objectives. The next step is risk assessment, which analyzes the severity level of these risks and their potential impact. The next step is concerned with the development of strategies to deal with risks, whether by avoiding, minimizing, transferring or appetizing risks. Risk management processes also include the establishment of monitoring and control mechanisms to ensure that risks are continuously monitored and the actions taken are evaluated. The final step is the continuous review and improvement of risk practices to ensure adaptation to changes in the internal and external environment of the entity. Figure (13) shows the most important procedures for risk management that must be available in the government entity.

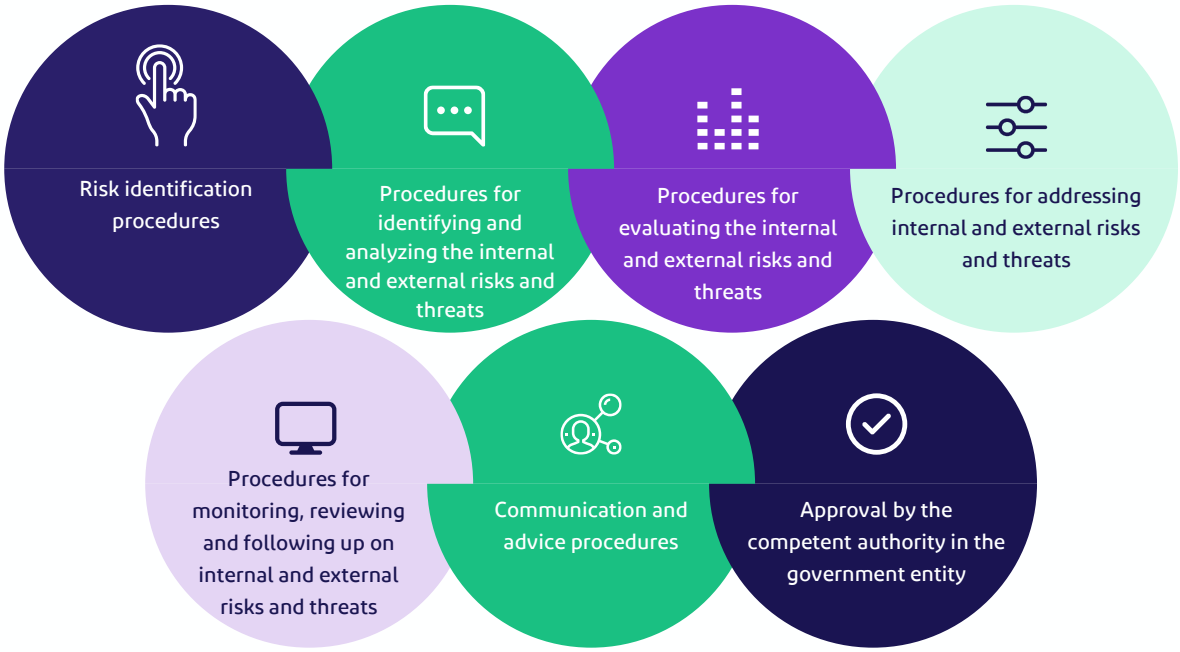


Figure (13): Risk Management Procedures

- Components of the Risk Management Procedures

The following section illustrates the main components of risk management procedures, as shown in Figure (14), followed by an explanation of each component:

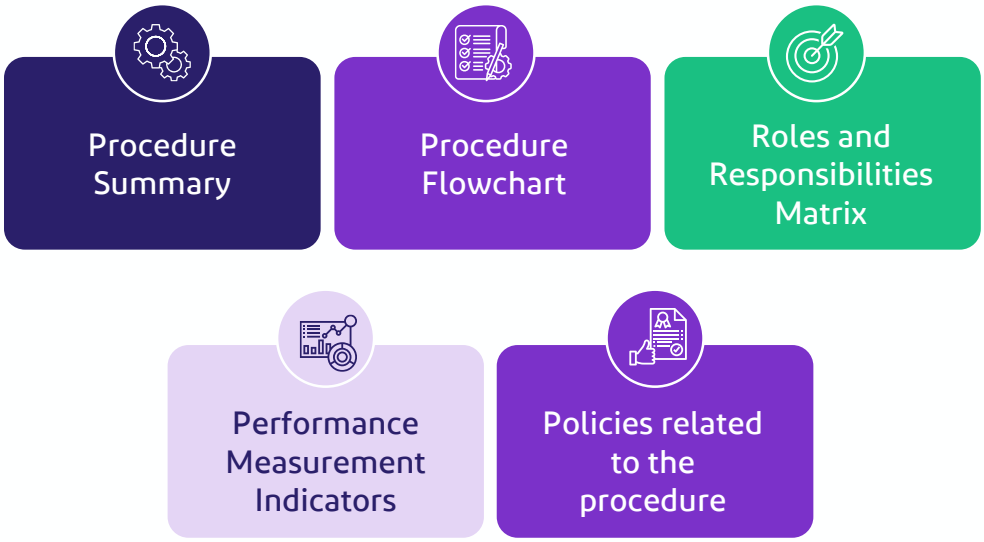


Figure (14): Components of the Risk Management Procedures

- **Procedure Summary**

A summary of the procedure is created, to include: Determining the name of the procedure, its purpose, description of the procedure, inputs and outputs, relevant stakeholders, as well as the systems used. This contributes to providing a comprehensive understanding of the procedure and effectively achieving the objectives of the government entity.

- **Procedure Illustrative Chart**

The procedure is outlined and explained through a flowchart, which illustrates the steps to be followed, the required tools, the activities specific to the procedure, as well as the relationship between activities, roles and responsibilities, and the outputs associated with each stage or activity, etc.

- **Roles and Responsibilities Matrix (RACI)**

The Roles and Responsibilities Matrix, which is an important tool for defining responsibilities and authorities between stakeholders and those involved in the procedure, is being developed. The Matrix includes the following:

- Activities Breakdown: The matrix describes all the activities carried out in the procedure, including the detailed steps and procedures for each activity.
- Linking activities to roles and responsibilities: The matrix identifies the roles to implement each activity in the procedure.
- Types of Authorities: The matrix identifies the types of authorities each official has, such as approval power, review power, or enforcement power.
- Service Level Agreement (SLA): The matrix sets out the Service Level Agreement (SLA) for each activity, which outlines the criteria that must be met when implementing the activity.

- **Performance Measurement Indicators**

A set of indicators that accurately reflect the performance of the stages and activities of the procedures are mentioned and clarified. These indicators include: Quality standards, time taken, efficiency, setting target values for each indicator, follow-up frequency, etc.

- **Policies associated with the Procedure**

The key policies associated with the procedure are outlined as a primary reference for the content, and are continually referenced to ensure that the procedure is properly applied, and in accordance with the specified standards. The key policies associated with a procedure can be a set of rules, principles or procedures that define how a procedure will be implemented.

5.1.5.1.4 Determining Risk Appetite and Tolerance Levels

Risk appetite and tolerance levels are an essential element of the success of risk management at the government entity. The administrative unit responsible for the risk management system works to establish risk appetite and tolerance levels guided by the strategic and operational objectives of the government entity. Risk appetite and tolerance levels are determined in cooperation with the executive management, stakeholders and stakeholders.

- Factors of Risk Appetite and Tolerance Levels

The strategic objectives, the internal and external scope of work, the internal and external stakeholders, the relevant legislation, laws and regulations, and the nature of previous risks to which the government entity was exposed shall be identified and clarified while determining risk appetite and tolerance levels, as shown in Figure (15):

1. Trends and expectations of the Board of Directors	2. Strategic pillars	3. Strategic objectives	4. External factors
Expectations or strategic trends are reflected by the Board in its identification of the risk appetite and tolerance levels.	They express the trend with regard to the current and expected future situation, and support the orientation of risk appetite in business and activities.	They are the basis for all operations. ERM must start by requesting a review and update of risk appetite and tolerance levels in the event of a change or modification in the strategic objectives.	The impact of economic factors, beneficiaries, laws and legislation, regulations, stakeholders, etc. is taken into account.
5. Internal Factors	**6. Potential Risks**	**7. Infrastructure**	**8. Risk Culture**
The current status of all internal components of the organization such as people, procedures, systems, policies, projects, risk tolerance, etc. are reviewed.	Potential risks that may affect the achievement of the strategic objectives are reviewed with stakeholders.	The available resources include automated tools, information systems, data, etc., which prepare administrative units to carry out their activities at the required level, and enhance the effective use of risk information.	A good risk culture enhances the effectiveness of risk appetite and tolerance levels, in terms of transparency in information sharing and awareness of the importance of taking intrinsic risks into account when making operational decisions and procedures.

Figure (15): Identification Factors of Risk Appetite and Tolerance Levels

Risk appetite vision and strategy varies from one side to another according to the directions of the board of the government entity and stakeholders, as shown in Figure (16):

Risk Averse	Any potential risks are avoided during the performance of the tasks or for achieving the objectives, meaning that the activities being carried out do not have any risks
Risk Cautious	The ability to carry out some tasks and activities that may result in a degree of risk to achieve the objectives, meaning that the activities being carried out may result in some controllable risks.
Risk Opportunistic	The ability to carry out tasks and activities that result in the greatest possible benefit to achieve the objectives with high risk, meaning that the activities being carried out may result in high risk in exchange for seizing opportunities.

Figure (16): Illustrative Example of Risk Appetite Trend Model

Figure (17) also shows the relationship between the risk appetite and tolerance levels, and context and scope of the government entity:

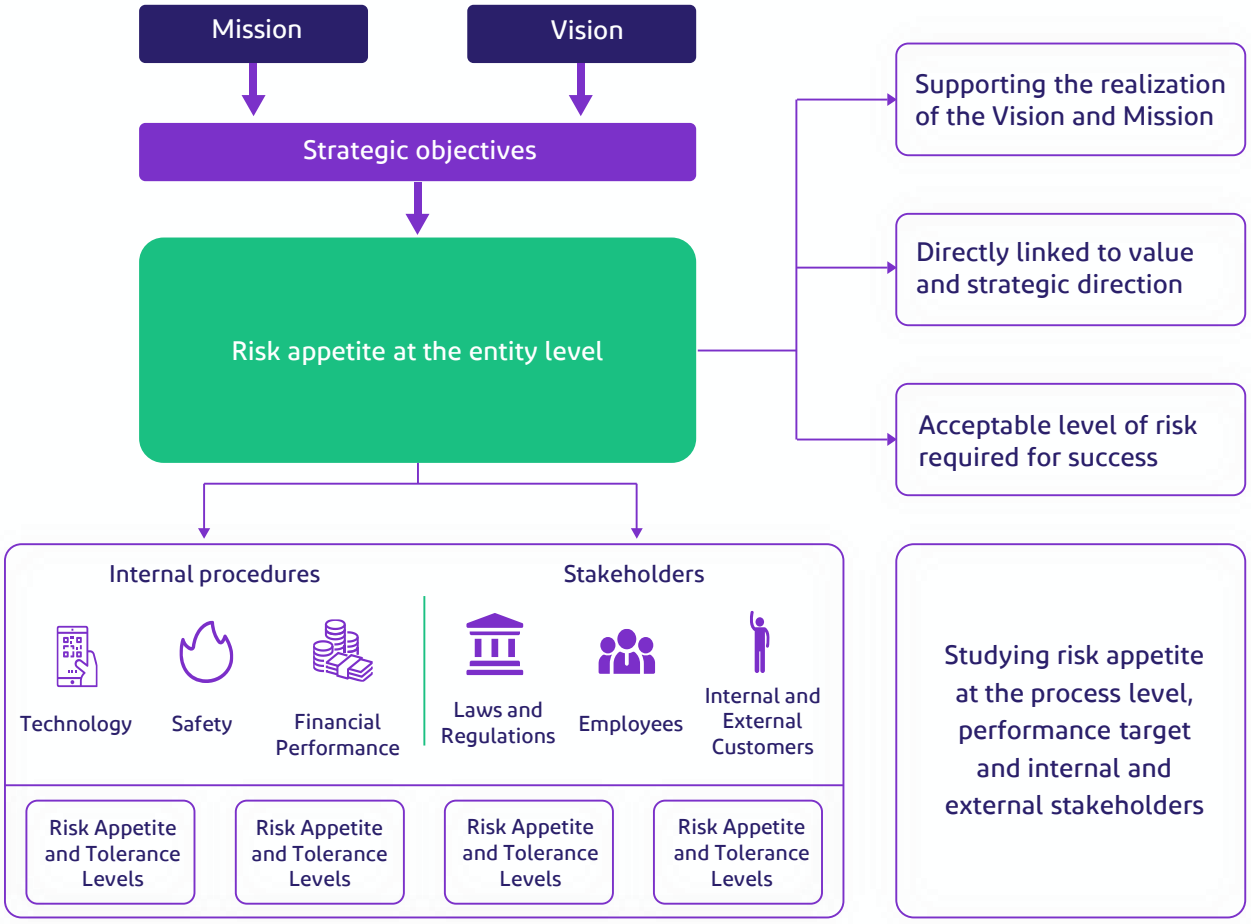


Figure (17): Relationship between the Risk Appetite and Tolerance Levels and the Government Entity Trend.

- Definition of Risk Appetite and Tolerance Levels

The values that define the governmental entity's approach to addressing potential risks are identified, relying on risk appetite and tolerance levels. Table (3) shows a model for defining risk appetite and tolerance levels.

Appetite Level	Acceptable Level	Tolerance Level
The value of the risks that the government entity is willing to accept without the need to implement continuous treatment, monitoring and follow-up plans.	The value of the risks that exceed the appetite limit, and the government entity has the ability to accept them with the need to implement continuous treatment, monitoring and follow-up plans.	The value of the risks that the government entity cannot accept to exceed, and requires the application of continuous treatment, monitoring and follow-up plans.

Correlation with the risk level assessment				
Ineffective	Low	Medium	High	Critical

Table (3): Definition of Risk Appetite and Tolerance Levels

- Escalation Mechanism of Risk Appetite and Tolerance Levels

To enhance and activate proactivity in addressing risks before they occur, a risk escalation mechanism is applied based on appetite and tolerance levels. Table (4) shows a model for the risk escalation mechanism of risk appetite and tolerance levels according to the levels.

#	Tolerance Level	Escalation Level	Procedure
1	Tolerance Level	Internal and external committees responsible for the Risk Management System.	Request support and take action to develop and implement treatment plans
2	Acceptable Level	The manager in charge of the administrative unit concerned with the risk.	
3	Appetite Level	Risk owner	No action required

Table (4): A Model for KRI Escalation Mechanism

- Identification Methods of Risk Appetite and Tolerance Levels

To ensure effective identification of risk appetite and tolerance levels, the government entity must adopt an integrated approach that includes a comprehensive review of a wide range of key elements and inputs to develop a thorough understanding of potential risks. By incorporating these inputs into the decision-making process, the entity can determine risk appetite and tolerance levels in a way that safeguards its interests and supports the efficient achievement of strategic objectives. Figure (18) highlights a set of the most important elements, including:

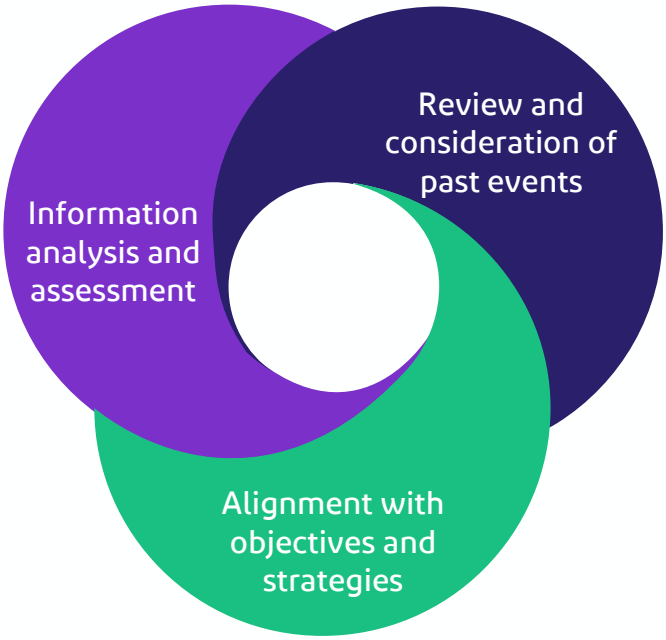


Figure (18): Identification Inputs of Risk Appetite and Tolerance Levels

Review and Consideration of Past Events: Referring to the previous recorded events, the historical features of the government entity, and the relevant situations and scenarios, to determine the limits of risk appetite and tolerance levels for future risks. This method can be considered one of the most important methods used to determine risk appetite and tolerance levels .

Information Analysis and Assessment Analyzing information from several different sources, such as: Conducting interviews with stakeholder, reviewing internal and external reports, and taking stakeholder feedback.

Alignment with Objectives and Strategies: Reviewing the government entity's strategy, analyzing its strategic objectives and pillars and performance measurement indicators, to determine the risk appetite and tolerance levels , in line with the stakeholders aspirations.

Components of the Risk Appetite and Tolerance Levels Document

The importance of governing risk appetite and tolerance levels lies in defining the review frequency, establishing mechanisms for monitoring and tracking risk appetite and tolerance level indicators, and determining the reporting frequency to the relevant committees and stakeholders. Figure (19) shows the Most Important Elements of Risk Appetite and Tolerance Levels.

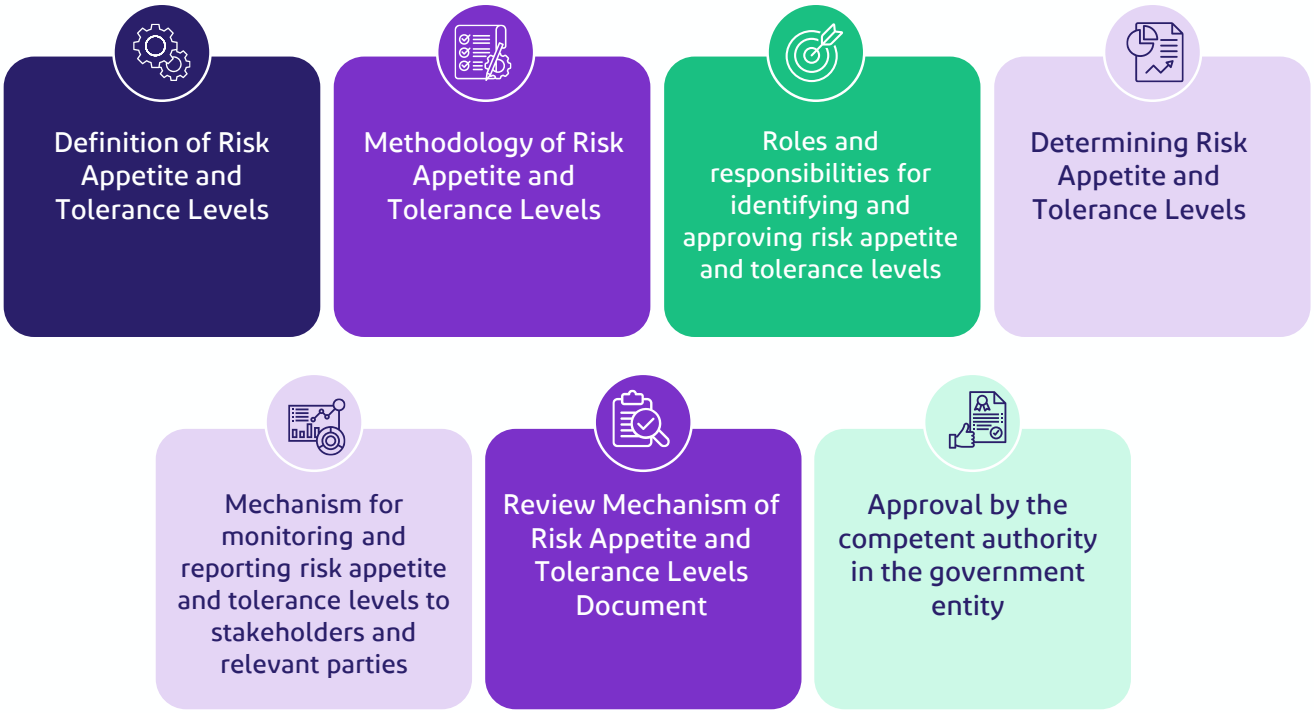


Figure (19): Most Important Elements of Risk Appetite and Tolerance Levels Document

- Definition of Risk Tolerance and Appetite Levels

The government entity's trend in addressing risks is clarified and determined by defining the risk tolerance and appetite levels Section (5.1.5.1.4) provides an illustrative example of risk appetite and tolerance levels model.

- Methodology of Risk Tolerance and Appetite Levels

The methodology used to determine the risk appetite and tolerance levels in the government entity is clarified and explained, with a focus on a systematic approach consistent with international best practices. Section (5.1.5.1.4) shows the most important methods used to determine risk appetite and tolerance levels.

- **Roles and responsibilities for identifying and approving risk appetite and tolerance levels**

The key roles and specific responsibilities of all stakeholders are clarified and defined, starting from senior management, through the managers of the concerned departments, Risk Champions, all the way to the risk management team. Emphasis is placed on cooperation and communication between different departments and stakeholders to ensure the effective exchange of information and views, and thereby contributing to achieving an accurate and objective assessment of risk appetite and tolerance levels.

- **Determining Risk Appetite and Tolerance Levels**

The risk appetite and tolerance levels in the government entity are clarified in a systematic and accurate manner, where the levels are carefully aligned with the strategic objectives of the entity and the directions of senior management. The analysis of the internal and external operating environment of the entity is taken into account, including economic, technological, political, and social changes and how these factors can impact risk appetite and tolerance. This analysis helps in guiding management decisions and strategic planning to ensure the efficient achievement of objectives while maintaining an acceptable level of risk. Section (5.1.6) shows the most prominent factors in preparing risk appetite and tolerance levels.

- **Mechanism for monitoring and reporting risk appetite and tolerance levels to stakeholders and relevant parties**

The use of a variety of advanced and effective tools is outlined to monitor and report on the risk appetite and tolerance levels within the government entity. The roles and responsibilities of all parties involved in this process are clearly defined, from department managers to stakeholders, to ensure accuracy and efficiency in collecting and analyzing risk-related data and information.

- **Periodic Review Mechanism of Risk Appetite and Tolerance Levels Document**

The mechanism of periodic review of risk appetite and tolerance level document shall be established and clarified in order to adapt the internal and external work environment and the changes to which the government entity is exposed.

- **Approval by the Competent Authority in the Government Entity**

The approval of the risk appetite and tolerance level by the competent authority at the government entity is documented upon the creation, as well as during periodic updates, to support the implementation of risk appetite and tolerance level document by all government entity's employees.

- **Key Risk Indicators (KRIs)**

A tool acts as an early warning system, and provides early warning of the consequences of potential adverse risks. They are measures used to identify and monitor risks that may affect the objectives of the government entity. They help to assess the likelihood and impact of risks and the effectiveness of actions taken to mitigate risks, and report, analyze and monitor any changes that may occur in key risk indicators periodically. Key risk indicators are determined based on risk appetite and tolerance levels. Key risk indicators can be classified into:

- Leading Indicators: Predictive indicators that measure the factors that contribute to predicting the occurrence of future risks. Such as: The number of hacking security systems and networks of the government agency.
- Lagging Indicators: Indicators that measure past events that may entail future risks. Such as: Number of critical system outages associated with major operations.

It is worth noting the difference between Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs), in terms of definition, purpose and significance. These Standards are shown in Table (5) below:

#	Standards	Key Risk Indicators (KRIs)	Key Performance Indicators (KPIs)
1	Definition	Measures used to monitor changes in the risk exposure level, and used as a means of an early warning of risks.	Measures used to evaluate performance and track progress toward achieving goals.
2	Purpose	Assessing potential risks and incidents that may affect the achievement of goals.	Measuring the effectiveness of business performance and achievement of strategic objectives.
3	Application Date	Used to predict and to warn of future risks.	Used to evaluate performance in a past or current period.
4	Identification and Review	Requires constant monitoring and regular adjustment based on the changing risk landscape.	They are identified annually and reviewed regularly (e.g., quarterly).
5	Focus	Focuses on potential threats and vulnerabilities.	Focuses on measuring performance, efficiency and success rates.
6	Alignment	Determined in alignment with the Entity's risk appetite and tolerance levels.	Determined in alignment with the strategic and operational objectives of the entity.
7	Responsibility	The Department responsible for Risk Management System.	The Department responsible for performance assessment.

Table (5): Comparison of KRIs and KPIs

Integrating key risk indicators with key performance indicators is essential to obtaining a comprehensive view of performance and risks within the government entity. This integration helps achieve a balance between striving to meet objectives and managing potential risks. Figure (20) shows the work mechanism of key risk indicators:

Figure (20): Work Mechanism of Key Risk Indicators:

Table (6) also provides examples of the KRIs Model:

#	Indicator	Description	Follow-up	Verification	Intervention	Monitoring Frequency
1	Number of critical technical service interruptions.	Number of critical system interruptions associated with major operations.	X times	x to x times	More than x times	Monthly
2	Speed detection of cyber-security incidents.	The time consumed to detect cyber incidents, and the average time taken to detect the incident after its occurrence in the government entity is calculated, as follows.	Less than x minutes	x to x minutes	More than x minutes	Monthly
3	Deviation in the achievement of strategic objectives and initiatives.	Measuring the percentage of deviation in achieving the targeted strategic objectives and initiatives.	X%	X% to x%	Less than x%	Yearly

#	Indicator	Description	Monitoring	Verification	Intervention	Monitoring Frequency
4	Number of digital fraud incidents.	Measuring the number of digital fraud incidents/cases detected and documented by the concerned parties.	X	x to x cases	More than x cases	Biannual
5	The hacking numbers of systems and networks.	Measuring the number of hacking security systems and networks of the government agency	Less than x attempts	x to x attempts	More than x attempts	Quarterly
6	Job Turnover Rate	Measuring the average turnover of the government entity's employees	Less than x%	X% to x%	More than x%	Biannual
7	Customers dissatisfaction of the services provided.	Measuring the percentage of customers' dissatisfaction with the services provided by the government entity through the questionnaires provided.	Less than x%	X% to x%	More than x%	Quarterly
8	Non-compliance with national laws and regulations.	Measuring deviation in achieving the targeted compliance rate of relevant national laws and regulations	Less than x%	X% to x%	More than x%	Quarterly

Table (6): KRIs Model

- Risk Champions Program

The Risk Champions Program aims to implement an effective organizational structure for the risk management system across the administrative units of the government entity. This ensures the communication and transfer of necessary knowledge regarding best practices in risk management, the adopted methodology, and the standards and tools used to those involved in risk management processes within the entity. Additionally, the program seeks to establish a network of risk representatives at the entity level.

- **Roles and Responsibilities of Risk Champions**

The roles and responsibilities of Risk Champions vary based on the current maturity level of risk management, and the extent to which the employees of the government entity are familiar with the risk management system. The primary role of Risk Champions is to act as a liaison between the administrative unit responsible for risks and the government entity's employees across all administrative units. Below is a clarification of the roles and responsibilities of Risk Champions, including, but not limited to:

- Collaborating with risk owners to identify and document changes and emerging risks specific to their departments.
- Supporting risk owners in establishing control measures and implementing risk treatment plans.
- Attending meetings and workshops for identifying, analyzing and assessing risks related to the concerned departments, and facilitating communication and collaboration on risk matters.
- Continuously monitoring and updating treatment plans within the relevant administrative units.
- Tracking risks and sharing updates of the risk register for the relevant administrative units with the unit responsible for risk management.
- Raising awareness and providing assistance to risk owners within their departments to adopt a proactive approach to risk management.
- Submitting periodic reports on the status of risks and updates related to risks to the administrative unit responsible for risk management.

- **Competencies and Skills of Risk Champions**

A Risk Champions document is developed to outline the administrative and technical skills required for fulfilling the role of Risk Champions, ensuring that responsibilities are carried out with the necessary efficiency. The Risk Champion for each administrative unit within the government entity is nominated in coordination between the relevant administrative unit and the unit responsible for risk management. Below are some of the key competencies and skills required for Risk Champions, including, but not limited to:

- Knowledge of the risk management methodology and practices adopted by the government entity, along with a willingness for continuous learning and development.
- The ability to effectively communicate with stakeholders and possess data analysis skills.
- Leadership, and strategic thinking and planning.

It is important for the Risk Pioneer to have the necessary authority to communicate and follow up with stakeholders regarding risks, as well as to monitor the risk registers of the relevant administrative unit.

- Components of the Risk Champions Document

The following section illustrates the main components of the Risk Champions Document, as illustrated in Figure (21), followed by an explanation of each component:

Figure (21): Components of the Risk Champions Document

- Introduction

An overview of the Risk Champions Program, the desired objectives and expected results of its implementation, the relevant roles and responsibilities, the required trainings, as well as the steps for implementing the program, and the program effectiveness.

- Criteria for Identifying Risk Champions and Required Competencies and Skills

A set of standards is identified and established to outline the key competencies and essential skills required for individuals' participation in this program. These standards include accurate risk analysis and assessment skills, the ability to think strategically and critically, and effective communication skills. Section (5.1.7) provides a detailed explanation of the key competencies and skills required for Risk Champions.

- **Roles and Responsibilities of Risk Champions**

The roles and responsibilities of Risk Champions are defined in a detailed and comprehensive manner in the risk management system of the government entity. Risk Champions are seen as key elements in the promotion and development of this system. Section (5.1.7) illustrates the most important roles and responsibilities of Risk Champions.

- **Required Trainings for Risk Champions**

The designed training programs and knowledge transfer methodologies are outlined to address the needs for enhancing the competencies and skills of Risk Champions within the government entity, ensuring the highest levels of performance and effectiveness. The training program includes educational content on global best practices in risk management, as well as materials aimed at developing the leadership and communication skills of Risk Champions. Training and knowledge transfer are delivered through various channels, such as e-learning, interactive sessions, practical exercises, specialized training, and workshops, all conducted by experts in the field. The training program is planned and approved in collaboration with the relevant departments within the government entity.

- **Steps for Implementing the Risk Champions Program**

The steps for implementing and executing the Risk Champions Program within the government entity are outlined, including detailed strategic planning, defining objectives and expected deliverables, and developing comprehensive action plans. Additionally, the roles and responsibilities of stakeholders and relevant parties are identified to ensure effective collaboration and the successful achievement of the program's intended goals.

- Risk Reporting System

The risk reporting system aims to enhance a risk-awareness culture, facilitate effective communication regarding risks, enable proactivity in addressing potential risks, and contribute to the continuous improvement of the government entity's risk management system by establishing a mechanism for reporting risks within the entity. A risk reporting document is created, which includes: The reporting mechanism and how to handle reports, related roles and responsibilities, and examples of a case study of reports, with an emphasis on ensuring the protection of whistleblower rights. Below are the key components of the risk reporting document.

- Components of the Risk Reporting Document:

- **Reporting Mechanism:**

Steps for reporting risks are established and clarified, starting with identifying and documenting risks, investigating risks, communicating risks with relevant parties, and ultimately addressing risks. This process includes outlining the available reporting channels to ensure efficient and effective communication of information, such as: internal portals, email, hotlines).

- **Reports Handling and Investigation:**

The initial risk assessment process is clarified, including communication with relevant parties, such as stakeholders and concerned departments, to ensure the exchange of essential data and information. The process emphasizes the actions taken to assess and address reported risks, maintaining confidentiality and neutrality during investigations, and ensuring unbiased evaluation of the situation and decision-making.

- **Roles and Responsibilities:**

The various and key roles of stakeholders and relevant parties are outlined, including the specific responsibilities of risk whistleblower, who play a vital role in identifying and notifying the government entity of any potential threats. The importance of the administrative unit responsible for the risk management system is also emphasized, as it undertakes the tasks of analyzing and assessing reported risks and developing appropriate response strategies.

The roles of risk owners and key related parties are clarified to ensure the implementation of necessary measures to mitigate those risks and prioritize actions. Additionally, the significance of the relationship between relevant parties throughout the risk reporting process lifecycle is highlighted, along with the mechanism for maintaining data and information confidentiality.

- **Risk Reporting Cases:**

The mechanism for monitoring risk reporting cases is detailed, including practical examples. Additionally, a distinction is made between whistleblowing, which typically involves reporting illegal or unethical behaviors or activities within the government entity, and risk reporting, which focuses on identifying suspected cases and threats that expose the government entity to potential losses, reputational damage, or other risks.

- **Protection Whistleblower Rights:**

The measures and actions implemented to ensure the privacy and confidentiality of whistleblowers' identities and the information provided in reports are outlined, aiming to protect them from any hostile behavior or negative discrimination within the government entity. These measures include enforcing privacy and security policies to ensure that whistleblowers' identities are not disclosed, thereby building trust in the reporting process.

- Key Deliverables of the Building and Governance of the Risk Management System

Based on the components and elements of the risk management system building and governance phase, Figure (22) illustrates the key deliverables of this phase, which are fundamental to the system's building.

Figure (22): Deliverables of the Building and Governance Phase of Risk Management

5.1.5.2 Activation of Risk Management Processes

This phase of the risk management lifecycle enables the government entity to identify risks, risk sources and consequences, as well as the controls currently in place. It also allows for the evaluation of inherent and residual risk levels. Additionally, it involves determining risk treatment strategies, monitoring risk status, and implementing treatment plans, as illustrated in Figure (23).

Figure (23): Activation of Risk Management Processes

- **Key/Principle Risks**

Key/Principle risks in the government entity are identified using either a Top-Down or Bottom-Up methodology. Key/Principle risks are monitored and tracked, and their reports are submitted to risk committees and stakeholders.

- **Top-Down Methodology**

A Top-Down methodology is applied to ensure that the Key risks facing the government entity are addressed in a strategic and integrated manner. Implementing this methodology requires a comprehensive and interactive vision from senior management and the board of directors, not only to identify risks but also to ensure the application of a risk-based approach in decision-making and in achieving the government entity's strategic objectives.

The following factors are considered to effectively implement the Top-Down Methodology:

1. Fostering a Risk Dialogue Culture: Enhancing discussions about risks among senior management, which helps achieve a clear understanding of potential risks facing the government entity and their impact on its strategic objectives.
2. Developing a charter that defines the roles and responsibilities of senior management concerning risks, along with the governance mechanism for communication and reporting related to the risk management system (e.g., the charter of the steering committee responsible for the risk management system).
3. Designing a dashboard tailored for senior management that provides a clear and direct view of the key risks and their potential impact on the entity's operations and strategic objectives.
4. Determining, publishing and applying the risk appetite and tolerance levels within the government entity.
5. Integrating risk management practices into the main operations of the government entity by identifying key processes and strategic objectives, pinpointing associated risks, and adopting a risk-based approach to address and manage thereof.

- **Bottom-Up Methodology**

The Bottom-Up Methodology is applied by gathering and analyzing information from the administrative units within the government entity to form a comprehensive understanding of the risks. This approach prioritizes the expertise of the entity's staff, and helps to identify potential risks at the entity level. The Bottom-Up Methodology is implemented through the operational risk department.

- Project Risk Management

The project risk management process enables government entities to proactively identify potential threats, challenges, and obstacles, and contributes to the improvement of project success opportunities, resource preservation, and ensuring the achievement of objectives within the specified timeline and budget. Figure 24 below provides a model of the project risk management methodology:

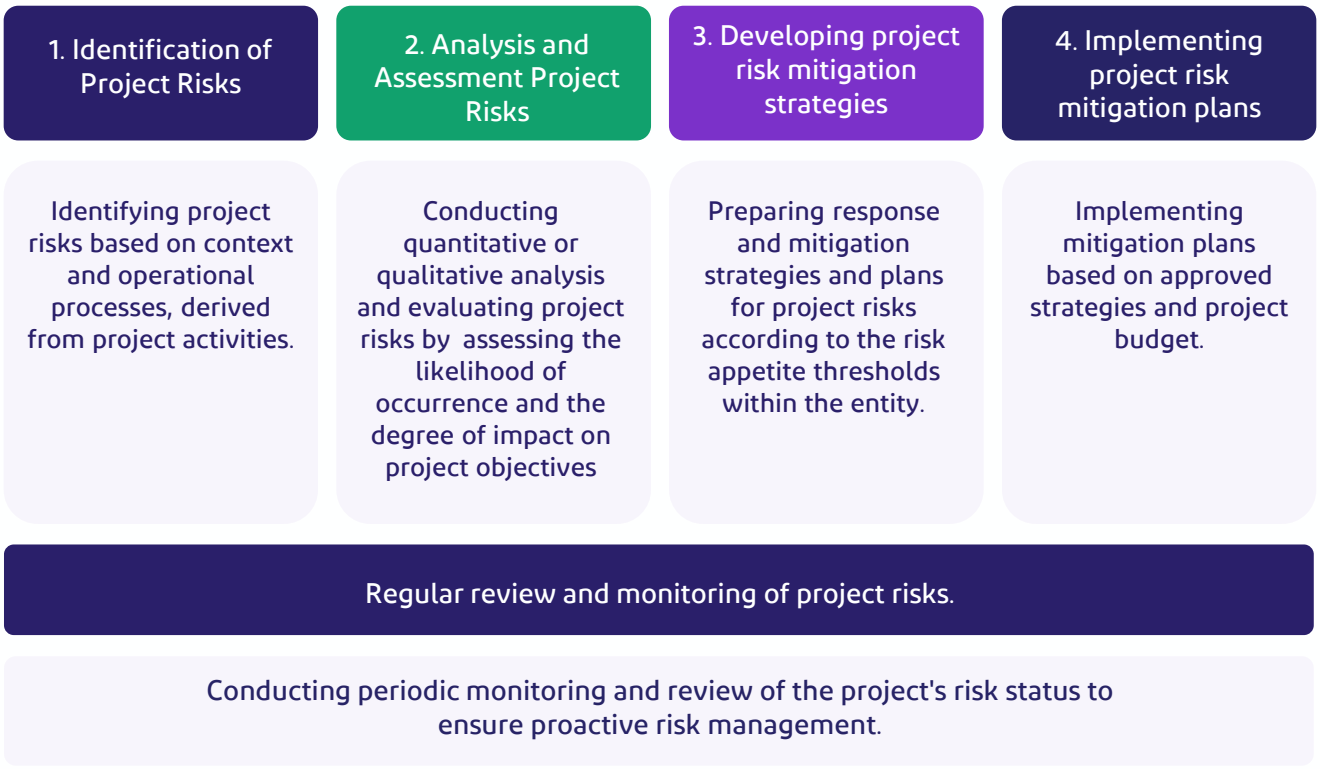


Figure 24 - Form of Project Risk Management Methodology.

- Processes Risk Management

Operational risk management contributes to identifying, analyzing, evaluating, mitigating, and monitoring various risks that may occur within the government entity and impact business performance and tasks, and thereby achieving the government entity's strategic and operational goals.

5.1.5.2.1 Risks Identification, Analysis and Assessment

An initial list of internal and external risks that may affect the government entity and hinder its ability to achieve its objectives is identified. This includes inputs from sources such as: Entity's historical data, theoretical analysis, expert inputs, risks from stakeholders, supply chain risks, and external and internal audit reports.

- **Risk Identification**

Risks are identified, classified and linked to the main and sub-risk categories defined and approved by the government entity, taking into account understanding and reviewing the operational objectives of the government entity's administrative units.

- Key Components of Risk Identification

- **Risk Identification Methods**

Risks are identified at the executive, administrative and operational level, through the implementation of the methods and techniques mentioned in Figure (25) below, which include, without limitation:

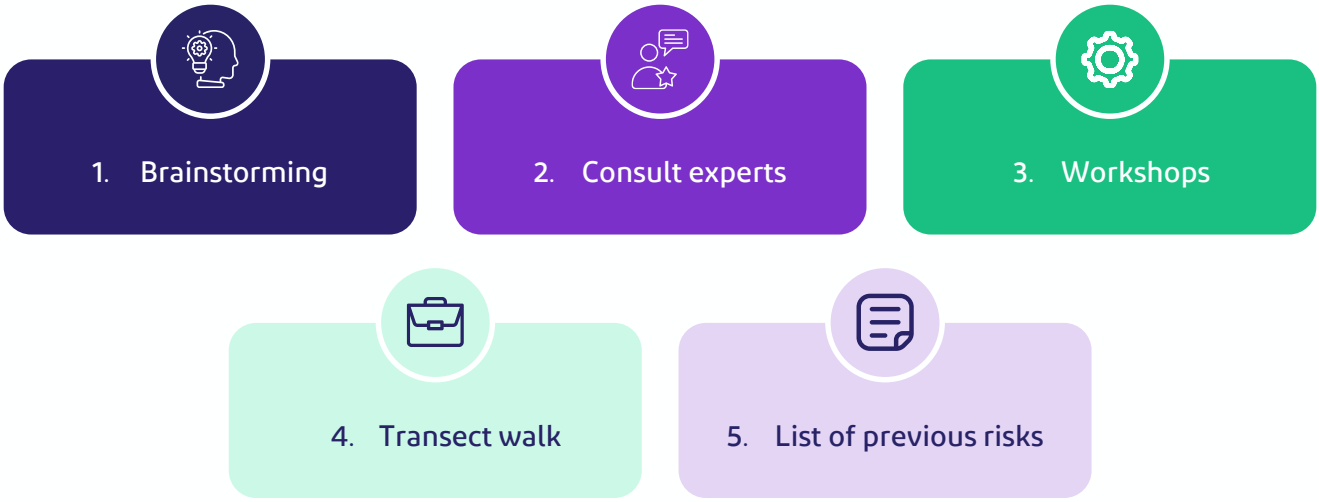


Figure (25): Risk Identification Methods

- **Documentation of Risk, Causes and Consequences**

Risks are clarified, formulated and written in a clear and concise manner that enhances the ability of stakeholders and relevant parties to accurately understand the different aspects of those risks. It also supports effective mitigation and proactive management of those risks. It also contributes to improving decision-making processes and enhances awareness and understanding of the importance of risk management in the context of achieving the strategic and operational objectives of the government entity.

- Clear risk descriptions (Figure 26) focus on identifying the potential event, its root causes, and the consequences of its occurrence. Potential risks can be linked to the targeted strategic and operational objectives of the government entity. A risk description is considered clear if it provides stakeholders with answers to the following questions:
- What could go wrong?
- Why could it happen?
- Why stakeholders should
- care about the incident?

Figure (26): Description of Risk Formulation

The risk is formulated in a single statement that includes the incident, causes and consequences, using the following formula:

(An incident that has an impact on the objectives) resulting from (cause/s) which may lead to (consequences/results))

Table (7) shows an illustrative example of risk formulation:

#	Incident	Causes	Consequences
1	Intervention with the performance of activities and businesses	• Lack of documented and approved policies and procedures. • Lack of clarity of roles and responsibilities of administrative units. • Lack of a matrix of roles and responsibilities for each administrative unit.	Conflict of interest and reputational impact.
2	Reduced operational resilience of digital services	• Lack of clear policies and procedures to ensure business resilience and sustainability. • Failure to apply business continuity controls in the technical structure. • Lack of periodic monitoring and review of the practices followed and controls applied. • Lack of service suppliers and resources to achieve operational flexibility.	Low beneficiary satisfaction percentage.

Table (7): Illustrative Example of Risk Formulation

- **Identification of Risk Owners and Risk Registration Date**

The person or administrative unit responsible for managing a particular risk shall be identified within its competencies and tasks, and the risk registration date shall be documented. The risk owner shall be responsible for following up the status of the risk and submitting the necessary reports to the unit responsible for the risk management system.

- **Classification of Main and Sub-Risk Categories**

The risks faced by the government entity are categorized into main and sub-risks, in alignment with its operational environment and scope of application. This approach helps to accurately understand and analyze the risks specified at the government entity level effectively and ensures proper reporting to stakeholders. Figure (27) provides an illustrative example of a model for the classifications of main risks and sub-risk categories.

Digital Risks

- Digital Fraud Risks
- Cloud Computing Risks
- Fixed and Intangible Assets Risks
- Infrastructure Risks
- Digital Transformation Risks

Strategic Risks

- Strategy and Planning Risks
- Reputation Risks
- Performance Indicators Risks
- Projects and Programs Risks
- Business Development Risks
- External Relations Risks
- Economic Risks
- Governance Risks

Legal and Compliance Risks

- Policy and Procedure Risks
- Legal Risks
- Fraud Risks
- Transparency and Control Risks
- Non-Compliance with National Laws and Regulations Risks.
- Roles and Responsibilities Risks
- Professional Conduct Risks

Operational Risks

- Operations Risks
- Assets Management Risks
- Human Resources Risks
- Supply Chain Risks
- Financial Risks
- Internal Technology Risks
- Business Disruption Risks
- HSSE Risks
- Business Continuity Risks

Cybersecurity Risks

- Data Confidentiality Risks
- Data Availability Risks
- Data Integrity Risks

Figure (27): Main and Sub-Risk Categories

- **Assistance Tools for Risks Identification:**

Potential risks and their root causes are identified. Based on the clear and precise understanding of these root causes, it facilitates the development of controls and mitigation plans for these risks. Risks and their root causes are identified using several methods, including:

- Ishikawa Diagram[4]

The Ishikawa Diagram, also known as the fishbone diagram or cause-and-effect diagram, is a graphical tool used to identify and analyze risks and the potential causes of a specific risk or impact. The Diagram (Figure 28) is constructed by identifying the risk or impact and then brainstorming potential causes that might contribute to this risk. These causes are categorized into various branches based on the fundamental factors they involve, such as: People, Processes, Technology, etc.

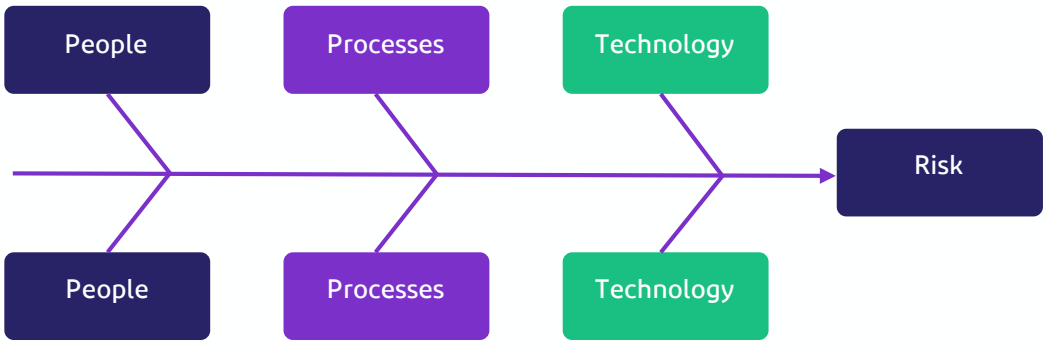


Figure (28): Ishikawa Diagram Model

[4]Referring to Reference No. (18) of Section (9. References and Sources.

Illustrative Example

#	Risk	People-Related Causes	Process-Related Causes	Implementation-Related Causes
1	Intervention with the performance of activities and businesses.	• Lack of awareness and adequate training for employees.	• Lack of policies and procedures for the administrative units. • Lack of roles and authorities matrices.	• Lack of automation of business procedures.
2	Reduced operational resilience of digital services	• Weak cooperation in the application of procedures.	• Ambiguity of roles and responsibilities	• Failure to apply business continuity controls in the technical structure.

Table (8): Illustrative Example of Ishikawa Diagram

- The Five Whys[5]

The five whys method is a technique used to identify the root causes of a risk. The method involves asking repeated "why" questions, usually five times to focus on the analysis and to identify the underlying causes of the risk, by continuing to ask the "why" question repeatedly. This method helps to identify deeper levels of the causes leading to the occurrence of the risk that may not be obvious at first. This method is simple and effective, and can help work teams quickly and systematically to identify the root causes, and thereby developing effective solutions (Figure 29).

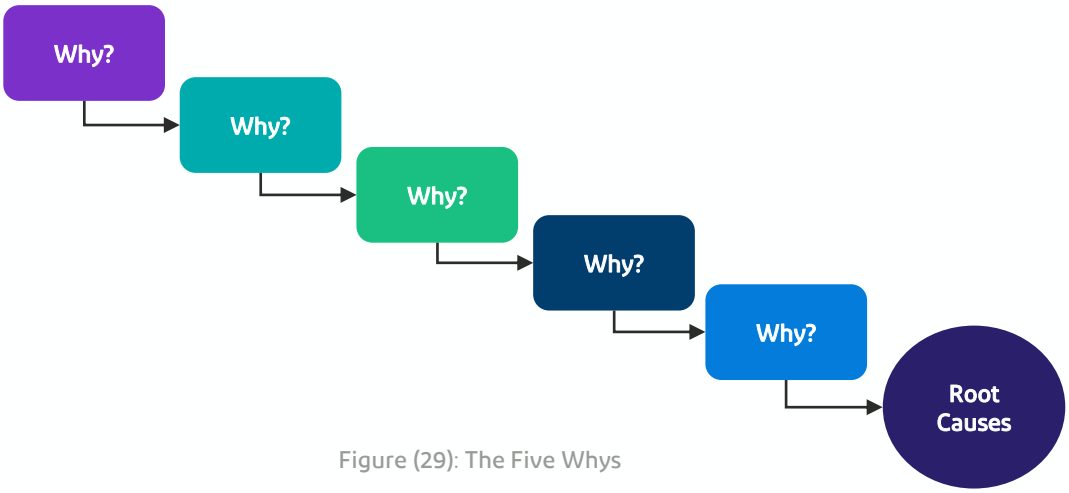


Figure (29): The Five Whys

Referring to Reference No. (18) of Section (9). References and Sources. [5]

Illustrative Example

- Risk: Reduced operational resilience of digital services.
- Why: Due to the inefficiency of the technical structure.
- Why: Due to weak controls in place to ensure continuity and recovery of systems.
- Why Due to lack of periodic monitoring and review.
- Why: Due to lack of clarity of relevant roles and and responsibilities.
- Why: Due to lack of clear policies and procedures to ensure business resilience and sustainability

- Risk: Intervention with the performance of activities and businesses.
- Why: Due to lack of clarity of roles and and responsibilities of the various administrative units.
- Why: Due to lack of a matrix of roles and authorities.
- Why: Due to lack of policies and procedures for the administrative units.
- Why: Due to the failure to build the organizational structure of all administrative units.
- Why: Due to poor strategic planning and lack of awareness among senior management.

Referring to Reference No. (3) of Section (9). References and Sources.[6]

- Bow Tie Diagrams[6]

The Bow Tie Diagram is used during risk assessment in risk analysis and identification of the risk root causes, as well as its consequences and results (Figure 30).

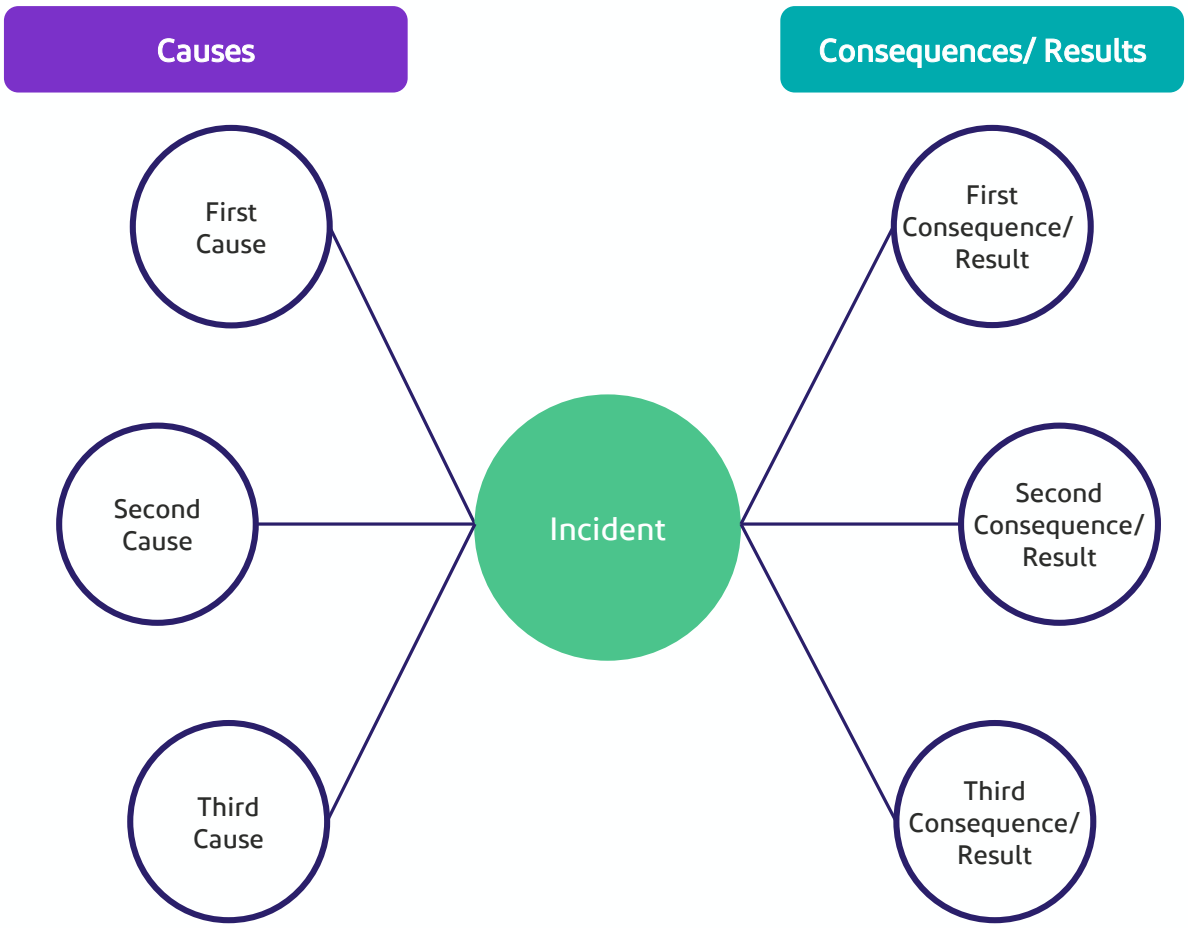


Fig 30: Bow Tie Diagram

Referring to Reference No. (3) of Section (9). References and Sources.[6]

Illustrative Example

#	Incident	Causes	Consequences
1	Intervention with the performance of activities and businesses	• Lack of documented and approved policies and procedures. • Lack of clarity of roles and responsibilities of administrative units. • Lack of a matrix of roles and responsibilities for each administrative unit.	• Conflict of interest. • Non-accountability. • Reputation impact.
2	Reduced operational resilience of digital services	• Lack of clear policies and procedures to ensure business resilience and sustainability. • Failure to apply business continuity controls in the technical structure. • Lack of periodic monitoring and review of the practices followed and controls applied. • Lack of service suppliers and resources to achieve operational flexibility.	• Frequent interruptions of services. • Low beneficiary satisfaction percentage. • Impact of realization of Saudi Vision 2030 goals.

Table (9): Analysis Bow Tie Diagram

- SWOT Analysis[7]

SWOT analysis is used as an analysis tool that enables and helps the government entity to identify and analyze potential internal and external risks. It assesses the strengths and weaknesses of the government entity, exploit opportunities, and deal with potential threats and risks. Figure (31) below shows The SWOT Analysis Form.

Strengths are the internal points of the entity that represent the features and resources that the entity has to reduce potential risks and help achieve objectives

Negative external conditions and factors that can threaten and hinder the achievement of objectives and cause potential risks.

Weaknesses are the internal points of the entity that need to be improved, developed and strengthened to reduce potential risks and achieve objectives

Positive external conditions and factors that can be exploited to achieve the objectives and reduce potential risks.

Figure (31): SWOT Analysis

[7]Referring to Reference No. (3) of Section (9. References and Sources.

- PESTEL Analysis[8]

PESTEL Analysis strategy is treated as an analysis tool used to help identify and analyze potential risks by analyzing six (6) key factors (Figure 32), namely: Political, economical, social, technical, environmental, and legal, and are considered an effective tool for strategic decision-making and predicting potential risks.

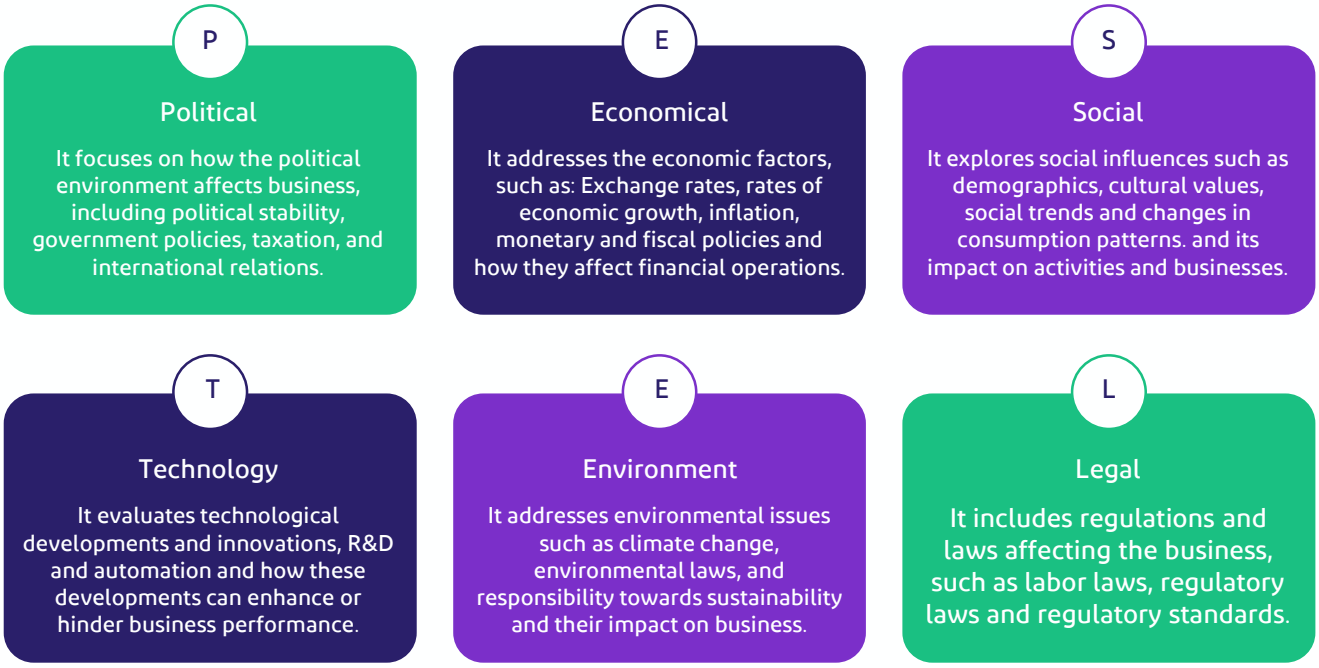


Figure (32): PESTEL Analysis

[8]Referring to Reference No. (3) of Section (9). References and Sources.

- Horizon Scanning[9]

The horizon scanning method is used as a proactive solution to explore future events. It contributes to achieving flexibility by identifying and monitoring the causes of change and emerging risks that may affect the government agency. It also helps to detect potential opportunities and threats resulting from the risks, which supports decision-making processes and correct planning to achieve strategic objectives. The following are the most prominent benefits of applying horizon scanning in the government entity:

- Collecting, analyzing and disseminating information to support decision-making.
- Better understanding the challenges and analyzing the extent to which the government entity is adequately prepared for potential opportunities and threats.
- Promoting advance preparedness for potential threats, risks and opportunities.

The Three Horizons Model (Figure 33) shows the level of incidents and the extent of their impact on the near and/or distant future in the government entity:

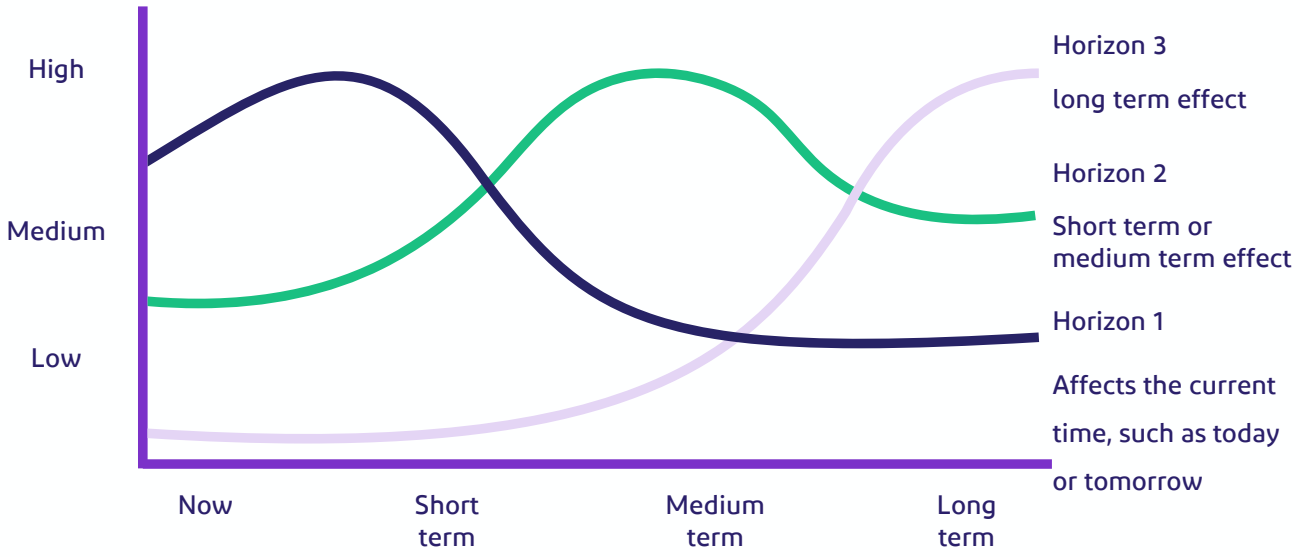


Figure (33): Horizon Scanning

- Horizon 1: what is being implemented at the moment.
- Horizon 2: Clear patterns to be considered in the near term.
- Horizon 3: There is little information at the moment, but advance planning is required.

Referring to Reference No. (7) of Section (9). References and Sources.[9]

- Horizon Scanning Steps:

The Form below (Figure 34) shows the steps that can be followed to conduct a horizon scanning:

Figure (34): Horizon Scanning Steps

- **Risk Analysis and Assessment**

Entity Risk Management Task Force conducts risk analysis in partnership with stakeholders, such as: Risk owners and Champions, operational teams, and others; in order to determine the expected effects on operations, and the impact on the objectives of the government entity as they occur. The predetermined risks are evaluated based on the impact and likelihood matrix prepared and approved by the government entity, which varies from one side to another according to the nature of its business and the types of expected impacts.

Referring to Reference No. (7) of Section (9). References and Sources.[9]

- Key components of Risk Analysis and Assessment

Assessment of Likelihood, Impact and Inherent Risk:

1. Likelihood: Likelihood is determined as shown in (Table 10). Expectations of occurrence/recurrence during the coming periods are also determined according to the nature of the government entity, and the effectiveness of the controls applied within the entity.

Likelihood Matrix		
Level	Frequency	Likelihood Ratio
1. Rare	It may only happen in exceptional circumstances, or it may happen once in two years.	Less than 10%
2. Unlikely	It is estimated that it is likely to occur about once or more than once in a year.	11% to 30%
3. Possible	It is estimated that it is likely to occur about twice or more in six months.	31% to 65%
4.Highly Likely	It is known to occur occasionally, at a rate of one or more times in 3 months.	66% to 89%
5.Almost Certain	Such incidents are expected to occur frequently, at a rate of one or more times within a month.	Over 90%

Table (10): Likelihood Matrix

2. **Impact:** The risk impact is evaluated based on the extent to which the risk, if it occurs, affects the government entity's strategies, objectives or operational processes, financial, operational, reputation, cybersecurity, human resources, legal / compliance, health, safety and security, etc. The variation in the main and subcategories of risks from one entity to another must be considered, depending on the nature and environment of the government entity's operations and the scope of application.

The following table provides a sample of impact matrix (Table 11) that includes examples of assessment levels and main risk categories:

Referring to Reference No. (7) of Section (9). References and Sources.[9]

Impact Matrix Model								
Level	HSSE	Financial	Operational	Reputational	Cybersecurity	Human Resources	Strategy	Legal/ Compliance
1. Ineffective	Little or no impact on buildings and safety and security of people (staff and customers); no need to evacuate the building; no injuries.	Insignific ant financial loss; less than x.	There is a limited level impact on the workflow, activities and systems of the Authority; non-critical services are disrupted for less than x minutes.	Less than x rise in partner or supplier complaints; from x to x negative social media post.	Possible indications that critical and /or supporting systems are the target of a cyber-attack or cybersecurity policy violations, resulting in internal leakage of classified (internal) data.	Less than x decrease from the targeted level of employee satisfaction ratios; the job dropout rate is less than x.	Slow progress in achieving one of the strategic goals of digital transform ation.	Not bound by any internal or external regulatio n, policy or provision.
2. Low	Minor impact on buildings and safety or security of people (staff and customers). Partial evacuation of the building without the need for third parties. Minor injury to one person requiring prompt medical attention.	Low financial loss; x to x.	The occurrence of an impact causing a minor disruption to the Authority's operations, activities, and systems. Non-critical services are interrupted for a duration of x to x minutes	From x to x rise in partner or supplier complaints; from x to x negative social media post.	Serious indications that critical and /or supporting systems are the target of a cyber-attack or cybersecurity policy violations, resulting in internal leakage of classified (confidential) data.	From x to x decrease from the targeted level of employee satisfaction ratios; the job dropout rate is from x to x.	Slow progress in achieving more than one strategic goals of digital transform ation.	It may be related to certain provisions of an internal regulatio n or policy; low legal penalties.
3. Moderate	Moderate impact on buildings and the safety or security of people (staff and customers). Complete evacuation of the building with the assistance of third parties, such as civil defense, with the possibility of returning to the building within two days. Multiple minor injuries requiring prompt medical attention.	Huge financial loss from x to x.	The presence of an impact that leads to a noticeable interruption in the workflow, activities and systems of the Authority for a short period; disruption of non-critical services for a period greater than x minutes; disruption of critical services for a period of x to x minutes without an impact on the main systems.	From x to x rise in partner or supplier complaints; from x to x negative social media post. Local media coverage for a duration of x to x days.	Attempts to hack critical and/or support systems with the aim of disrupting or tampering with them, resulting in external leakage of classified (internal) data, or leakage of source code.	From x to x decrease from the targeted level of employee satisfaction ratios; the job dropout rate is from x to x.	Disruptio n of one of the strategic goals of digital transform ation.	Only linked to internal regulatio n, policy or provisions ; placing operation al processes under internal supervisio n; significan t legal penalties.

Impact Matrix Model								
4. High	Significant impact on buildings and the safety or security of people (staff and customers). Complete evacuation of the building with the assistance of third parties, such as civil defense, with the possibility of returning to the building within a week, with injuries.	Significant financial loss from x to x.	The occurrence of an impact causing a notable disruption to the Authority's operations, activities, and systems. Critical services are interrupted for a duration of x to x minutes, and key systems are also affected.	From x to x rise in audience, partner or supplier complaints; from x to x negative social media post. Negative post by social media influencers. Local media coverage for a duration of x to x days.	Attempts to hack critical and/or support systems with the aim of disrupting or tampering with them, resulting in an impact on the service availability, or external leakage of classified (confidential) data.	From x to x decrease from the targeted level of employee satisfaction ratios; the job dropout rate is from x to x.	Disruption achieving more than one strategic goals of digital transformation.	Linked to external regulation, policy or provisions; placing operational processes under supervision of external regulatory authority.
5. Critical	A very significant impact on buildings and the safety or security of people (staff and customers). Complete evacuation of the building with the assistance of external entities, such as Civil Defense. The building becomes unusable in the near future; and the occurrence of loss of life.	A very huge financial loss; more than x.	The occurrence of an impact causing a notable disruption to the Authority's operations, activities, and systems for a long period. Critical services are interrupted for a duration more than x minutes, and key systems are also affected.	More than x rise in partner or supplier complaints. More than x negative social media post. Several negative post by social media influencers. Local and global media coverage.	Attempts to hack critical and/or support systems with the aim of disrupting or tampering with them, resulting in a destructive impact on the service availability, or external leakage of classified (very confidential) data, or external leakage of source codes.	More than x decrease from the targeted level of employee satisfaction ratios; the job dropout rate is greater than x.	A decline in the achievement of one or more of the strategic digital transformation objectives or a threat of failure of the strategic plan.	Linked to a material regulation, policy or basic external provisions; the cessation of operations by regulators.

Table (11): Impact Matrix Model

3. Risk Assessment Matrix: A numerical and/or descriptive risk value is estimated, using a risk assessment matrix or heat map. The risk assessment matrix contributes to the qualitative and quantitative risk analysis and increases the quality of decision-making related to the importance of risk and the priority of treatment plans. There are several ways to present the risk matrix (Table 12). The assessment matrix is designed using the likelihood and impact levels of the government entity. There are types of assessment matrix, such as: (Triple matrix, quadruple matrix, and pentamatrix).

Table (12) shows a model of a pentamatrix, as the most used matrix in risk assessment:

Risk Assessment Matrix Model					
Likelihood	Impact				
	1. Ineffective	2. Low	3. Medium	4. High	5. Critical
5. Almost certain	5	10	15	20	25
4. Highly Likely	4	8	12	16	20
3. Possible	3	6	9	12	15
2. Likely	2	4	6	8	10
1. Rare	1	2	3	4	5

Table (12): Risk Assessment Matrix Model

4. Inherent Risk: Risks that the government entity faces before taking any mitigation action or assessment of controls. The risk likelihood and impact are measured without taking into account the effectiveness of controls. Figure (35) shows a model for the method of calculating the degree of inherent risk:

Figure (35): Inherent Risk Calculation Method

Applied Controls

Procedures and controls that are implemented on systems, applications networks or the work environment, through which risks that are likely to occur are mitigated or reduced. Controls are divided into several classifications, such as:

- **Preventive Controls**

Controls that are designed and implemented to identify deviations before they occur, and take appropriate action to prevent these deviations, such as: (Segregation of duties, binary control, passwords for access to operating systems and applications).

- **Detective Controls**

Controls that are designed and implemented to detect errors and deviations when they occur. Detective Controls are very important to measure the efficiency of preventive controls. The application of these controls is more expensive than the application of preventive controls. Such as: (Audit logs issued from applications, systems, and surveillance cameras).

- **Corrective Controls**

Controls that are designed and implemented to ensure that corrective actions for deviations have been implemented, or that these deviations have not occurred again. This category of controls is complementary to the previous types, as it addresses deviations and errors that exceeded the preventive controls and were detected through the detective controls. Such as (recovering data from backup means).

- **Deterrent Controls**

Controls that serve as a deterrent for individuals to carry out any deviations or excesses that may cause risks and affect the objectives of the government entity. Such as (conducting an independent internal audit, having a violation regulation, and guarding some sensitive sites, such as data centers).

Assessing the effectiveness of controls applied:

The effectiveness of the applied controls is measured and the relative score of the effectiveness of the applied control is evaluated, and used to calculate the residual severity. Table (13) shows an example of the model for measuring the effectiveness of the controls applied in the government entity:

#	Evaluation	Description	Examination of control effectiveness	Relative score of control effectiveness measurement
1	No control	No controls have been implemented or activated to reduce the likelihood or impact of a risk.	No sample for examination	0%
2	Ineffective	The control has not been designed effectively, is incorrectly applied, or is causing new risks.	Supervisory control is not applied	15%
3	Requires improvement	The control is designed and implemented to a simple degree with gaps that require improving and raising its effectiveness.	The control is partially applied	50%
4	Partially effective	The control is designed and implemented with a high degree of efficiency, with some points of improvement.	The control is almost fully implemented	70%
5	Very effective	The control is designed and implemented with the required efficiency and effectiveness.	The control is fully and regularly implemented	90%

Table (13): Assessing the Effectiveness of Controls Applied

Assessment of Residual Risks

Residual Risk: The likelihood and impact of the residual risk or degree of risk is measured after taking into account the effectiveness of the controls applied. Figure (36) below provides a model for calculating the degree of residual risk:

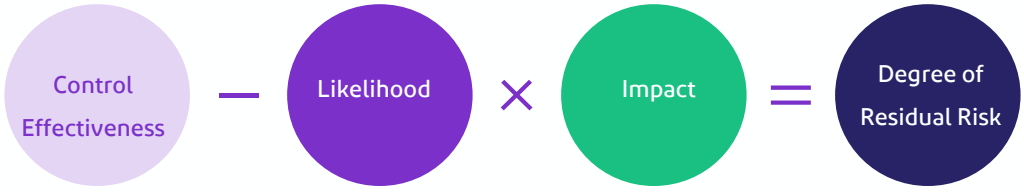


Figure (36): Residual Risk Calculation Method

Risk Velocity

Risk velocity is used to help prioritize the identified risks in the event that the impact and likelihood are of the same value. Risk velocity depends on measuring the amount of vulnerability of the government entity when it is exposed to the risk, which is the time between the occurrence of the incident and the phase at which the government entity is affected by the incident consequences. Risk degree is calculated if we consider risk velocity as indicated in Figure (37) below:

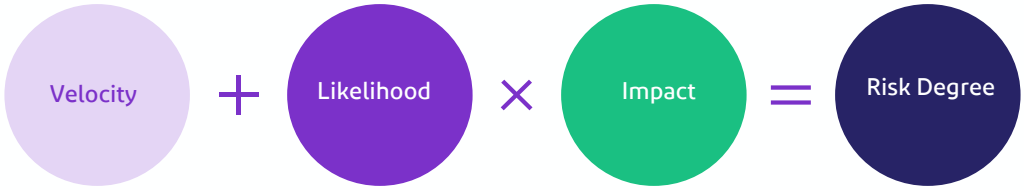


Figure (37): Risk Velocity Calculation Method

Table (14) below shows examples of the classification of risk velocity and duration for each category:

Classification	Description	Velocity
5	Extremely High/ Critical	Direct
4	Elevated/ High	More than a day to one month
3	Average	More than one month to three months
2	Low	More than three months to twelve months
1	Extremely Low/ Unaffected	More than a year

Table (14): Risk Velocity Classification

Illustrative Example

The following example illustrates the risk analysis method, taking into account risk velocity:

When using the traditional analysis method of "interference in the performance of activities and business, which may lead to conflicts of interest and reputational impact" mentioned in Table (12), which consists of only two factors in calculating the degree of risk (likelihood and impact), the likelihood is determined at "4". The impact is determined at "4". The inherent risk degree is determined at "16".

Risk Velocity Assessment

Using the Risk Velocity Scale. We can conclude that risk velocity can occur in more than one day to one month, and therefore the Risk Velocity was determined as “High (4)”. The inherent risk degree is determined at “Critical (20)”.

Table (15) shows the application of risk velocity assessment to the example shown:

Risk	Likelihood	Impact	Velocity	Risk Assessment
Intervention with the performance of activities and businesses	Probable (4)	Critical (4)	High (4)	Critical (20)

Table (15): Risk Velocity Assessment

Illustrative Example

Table (16) below provides an example of a risk analysis and assessment process:

#	Risk Description	Risk Causes	Inherent Impact Assessment	Inherent Likelihood Assessment	Inherent Risk Degree	Applied Controls	Controls Effectiveness Assessment	Residual Risk Degree
1	Intervention with the performance of activities and business due to lack of documented and approved policies and procedures, thereby resulting in conflicts of interest and reputational damage.	1. Lack of documented and approved policies and procedures. 2. Lack of clarity of roles and responsibilities of administrative units. 3. Lack of a matrix of roles and responsibilities for each administrative unit.	High (4)	Probable (4)	High (16)	1. Policies and Procedures for Administrative Units	(3) Requires improvement	(12) Moderate
2	Decreased operational resilience of digital services due to the lack of clear policies and procedures to ensure business resilience and sustainability, thereby reducing beneficiary satisfaction.	1. Lack of clear policies and procedures to ensure business resilience and sustainability. 2. Failure to apply business continuity controls in the technical structure. 3. Lack of periodic monitoring and review of the practices followed and controls applied. 4. Lack of service suppliers and resources to achieve operational flexibility.	(3) Moderate	(4) High	(12) Medium	No controls applied	(0) N/A	(12) Moderate

Table (16): Illustrative Example of Risk Identification, Analysis and Assessment

- **Risk Self-Assessment and Applied Controls10**

The self-assessment method aims to consolidate the risk-based approach in the operational processes at the government entity level. It contributes to determining exposure and exposure to risks, and evaluating the effectiveness of the applied controls, thereby facilitating the process of identifying priorities, gaps and weaknesses. The design of the self-assessment methodology takes into account the unnecessary complexity, which in turn makes it difficult to complete tasks and negatively affects the achievement of the strategic objectives of the government entity.

Self-assessment is carried out by risk owners, and there are many methods that can be applied to carry out self-assessment. The government entity must take into account the nature of the work environment and the volume of business, as well as its risk culture. The following section clarified, for example, but not limited to, the most important methods used to implement self-assessment:

- Workshops Self-assessment through workshops aims to ensure interaction with risk owners and the transfer of knowledge about risks by those responsible for risks, which contributes to enhancing the risk culture in the government entity.
- Questionnaires: Questionnaires are used as an alternative to the workshops to collect the information required to implement the self-assessment, and to reach as many risk owners as possible in a timely manner. It contributes to determining exposure and exposure to risks on a larger scale in the government entity.

- Qualitative and Quantitative Risk Assessment[11]

Risks are evaluated using quantitative or qualitative analysis of potential risks that the government entity may face. The evaluation method suitable for the maturity level of risk management system practices and the current working environment within the government entity is utilized. Table (17) provides a comparison between the qualitative and quantitative evaluation methods:

#	Factors	Qualitative Assessment	Quantitative Assessment
1	Application	• In the absence of sufficient risk data. • In case of emerging risks. • In case expert opinions and stakeholder input are needed.	• In case sufficient risk data is available. • In the case of being able to measure risk inputs based on clear and accurate figures.
2	Work Mechanism	Analyzing and assessing risk based on experience, intuition and knowledge that is not necessarily based on quantitative data.	Risk analysis based on accurate analyses and calculations to analyze and evaluate risks in clear numbers.
3	Implementation	By conducting interviews and workshops with stakeholders, and using impact, likelihood and risk severity matrices.	By using statistical tools and models, such as: Monte Carlo analysis, annual loss forecast analysis, based on analytical data and probabilistic analysis.

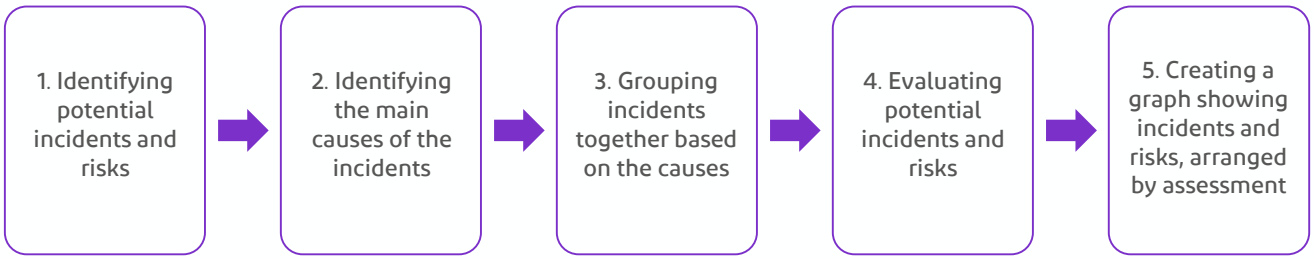
Table (17): Quantitative and Qualitative Risk Assessment

[11] Referring to Reference No. (3) of Section (9). References and Sources.

- Pareto Principle (The 80/20 Rule)[12]

The Pareto Principle is used as an analysis tool to highlight the most important factors or triggers of risks. The Pareto Principle is based on The 80/20 Rule, an idea that 20% of the causes result in 80% of the incidents, or that by doing 20% of the business, 80% of the expected results can be achieved. This Principle helps prioritize and assess the severity of the identified risks.

The Pareto Principle is created by implementing the following steps shown in Figure (38):



Pareto Principle

Figure (39) below provides an illustrative example showing the relationship between potential threats or risks and their associated causes, for example: 37% of the root causes constitute 63% of the potential risks.

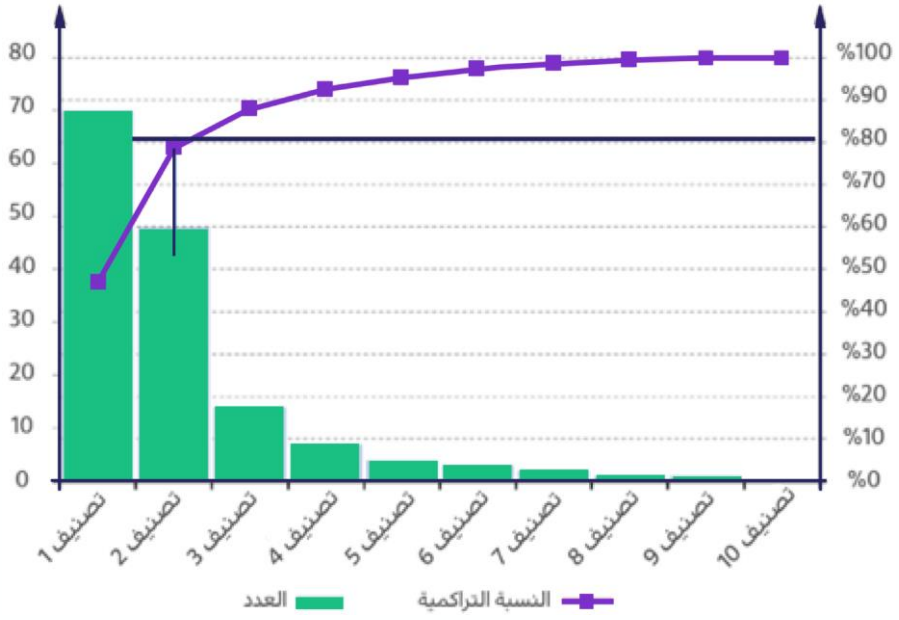


Figure (39): Relationship between Threats and Risks

[12]Referring to Reference No. (3) of Section (9). References and Sources.

- **Value at Risk (VaR)**

Value at Risk (VaR) is an indicator of the amount of potential financial loss in the financial assets portfolio over a specified period of time, with a specified probability ratio (confidence level). They can be used to assess risk at the level of a single asset or an entire investment portfolio. The value at risk is used to answer the following question: What is the worst expected financial loss in a given period of time? What is the level of confidence in the likelihood of that loss?

The value at risk is determined using three (3) methods, namely: Historical factors, covariance method, and Monte Carlo simulation:

- Historical Factors: Assuming a repetition of historical events, the value at risk is calculated using historical values and returns from bad to better over a specified period of time.
- Covariance Method; Past historical values and returns are used, setting hypothetical values by averaging values and the difference between them, to determine the value at risk over a specified period of time.

Monte Carlo Simulation: Historical values and returns are used to create a number of possible scenarios using technological tools and computational models, and to repeatedly analyze those results for various variables over a specified period of time to reach the value at risk.

For example: Assuming that the value of the asset portfolio is 100 million, if the value at risk of1.16 million during a month equals 99% (that is, the probability of exceeding 1.16 million during the specified period is 01%).

5.1.5.2.2 Risk Treatment

Appropriate risk treatment plans are developed after identifying, analyzing and evaluating the risks, to reduce the negative impact of the risks on the achievement of the government entity's objectives or to exploit the opportunities resulting from the risks. To effectively design risk treatment plans, the feasibility analysis of addressing the risk is carried out, and the methodology and strategy for dealing with each risk are identified based on the risk appetite and tolerance levels. Detailed response plans are developed, prioritized, and approved according to authority levels.

- Key Components of Risk Treatment

Risk Treatment Strategies

The measures taken by the government entity to deal with the negative risks that may affect the objectives. Figure (40) shows the strategies for addressing / dealing with risks:

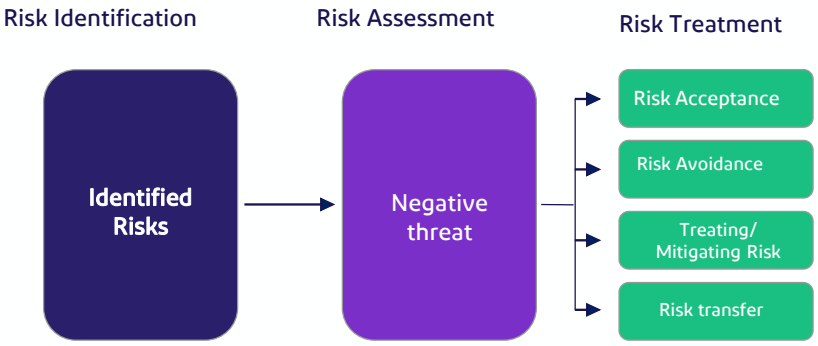


Figure (40): Risk Handling Strategies

1. **Risk Acceptance:** Accept risks without adding additional controls to reduce the impact and likelihood of risks.

Considerations:

- If the impact resulting from the risk is less costly than the application of controls or treatment plans.
- If the risk severity falls within the risk appetite level.

2. **Risk Avoidance:** Suspension of certain tasks, operational processes, or activities, which resulted in the risk.

Considerations:

- If it is not possible to reduce the impact or the likelihood of risks within the government entity.
- If the avoidance of risk does not have a direct impact on the achievement of any of the strategic or operational objectives of the government entity.

3. **Risk Mitigation/Treatment**: It includes the implementation of additional controls and treatment plans in order to reduce the likelihood of the risk and the extent of its impact on the government entity.

Considerations:

- If the risk severity is higher than the risk appetite level.
- If the risk has a direct impact on the achievement of any of the strategic or operational objectives of the government entity.

4. **Risk Transfer**: Reducing impacts and likelihood by sharing the risk or part of it with third parties.

Considerations:

- If the risk transfer cost is less costly than the application of controls or treatment plans.

Governance of Treatment Plans

The governance mechanism of treatment plans clarifies the period that the government entity's employees should adhere to in order to implement the proposed risks treatment plans. The specified period varies according to the remaining risk severity. Table (18) below provides an illustrative example of the governance model of risk treatment plans:

#	Risk Severity	Maximum duration for implementing treatment plan	Ability to modify treatment plan date
1	Critical	3 months	One month from the date of the initial approval with a notification to the risk committees before modifying the date.
2	High		
3	Moderate	6 months	2 months from the date of initial approval
4	Low	12 months	4 months from the date of initial approval
5	Ineffective		

Table (18) below provides an illustrative example of the governance model of risk treatment plans

Table (19) below provides an illustrative example for identifying risk treatment plans: [13]

[13]The above figures and ratios are for reference only, and are not an accurate representation of the reality of any particular entity. A detailed study of the current situation of the entity shall be conducted, and acceptable levels shall be determined for each of them, in accordance with the work environment and nature of the entity.

#	Risk Description	Risk Causes	Inherent Risk Degree	Applied Controls	Controls Effectiveness Assessment	Residual Risk Degree	Treatment Plans	Targeted Date
1	Intervention with the performanc e of activities and business due to lack of documente d and approved policies and procedures, thereby resulting in conflicts of interest and reputational damage.	1. Lack of documented and approved policies and procedures. 2. Lack of clarity of roles and responsibilities of administrative units. 3. Lack of a matrix of roles and responsibilities for each administrative unit.	(16) High	1. Policies and Procedur es for Administ rative Units.	(3) Requires improve-ment	(12) Mode rate	1. Identifying and documenting the roles and responsibilities of the administrative units. 2. Identifying and documenting the authority matrix for the policies and procedures of the administrative units.	4 months
2	Decreased operational resilience of digital services due to the lack of clear policies and procedures to ensure business resilience and sustainabilit y, thereby reducing beneficiary satisfaction.	1. Lack of clear policies and procedures to ensure business resilience and sustainability. 2. Failure to apply business continuity controls in the technical structure. 3. Lack of periodic monitoring and review of the practices followed and controls applied. 4. Lack of service suppliers and resources to achieve operational flexibility.	(12) Moderate	No controls applied	(0) N/A	(12) Mode rate	1. Creating an IT governance model. 2. Developing business continuity plans 3. Establishing a technology architecture strategy to ensure business resilience and sustainability. 4. Providing the necessary resources (technological, human, financial, etc.) to achieve operational flexibility.	9 months Moderate

Table (19): Identification of Risk Treatment Plans

Assistance Tools for Risk Treatment:

Multi-Criteria Analysis (MCA)14

Multi-criteria analysis uses a set of criteria to assess and compare the overall performance of a set of options with complete transparency. It aims to determine the importance and priority of those options. The analysis involves creating a matrix of factors and criteria that are ranked and grouped to provide an overall score for each option. Multi-criteria analysis is used to prioritize risk treatment plans, thereby contributing to saving resources and costs for government entities. Multi-criteria analysis is implemented by

following the below steps as shown in Figure (41):

Figure (41): Multi-Criteria Analysis

[14]Referring to Reference No. (3) of Section (9). References and Sources.

Cost-Benefit Analysis15

Cost-benefit analysis at the strategic and operational level is used to support decision-making and optimal allocation of resources and capabilities when defining risk treatment strategies, as well as when developing risk treatment plans. The analysis begins by identifying potential risks and considering different options for addressing them. This includes estimating the costs associated with each option, as well as evaluating the expected benefits, with the aim of choosing the solution that offers the best balance between costs and benefits, taking into account the relevant standards and regulations. The cost-benefit analysis is carried out by following these steps (Figure 42):

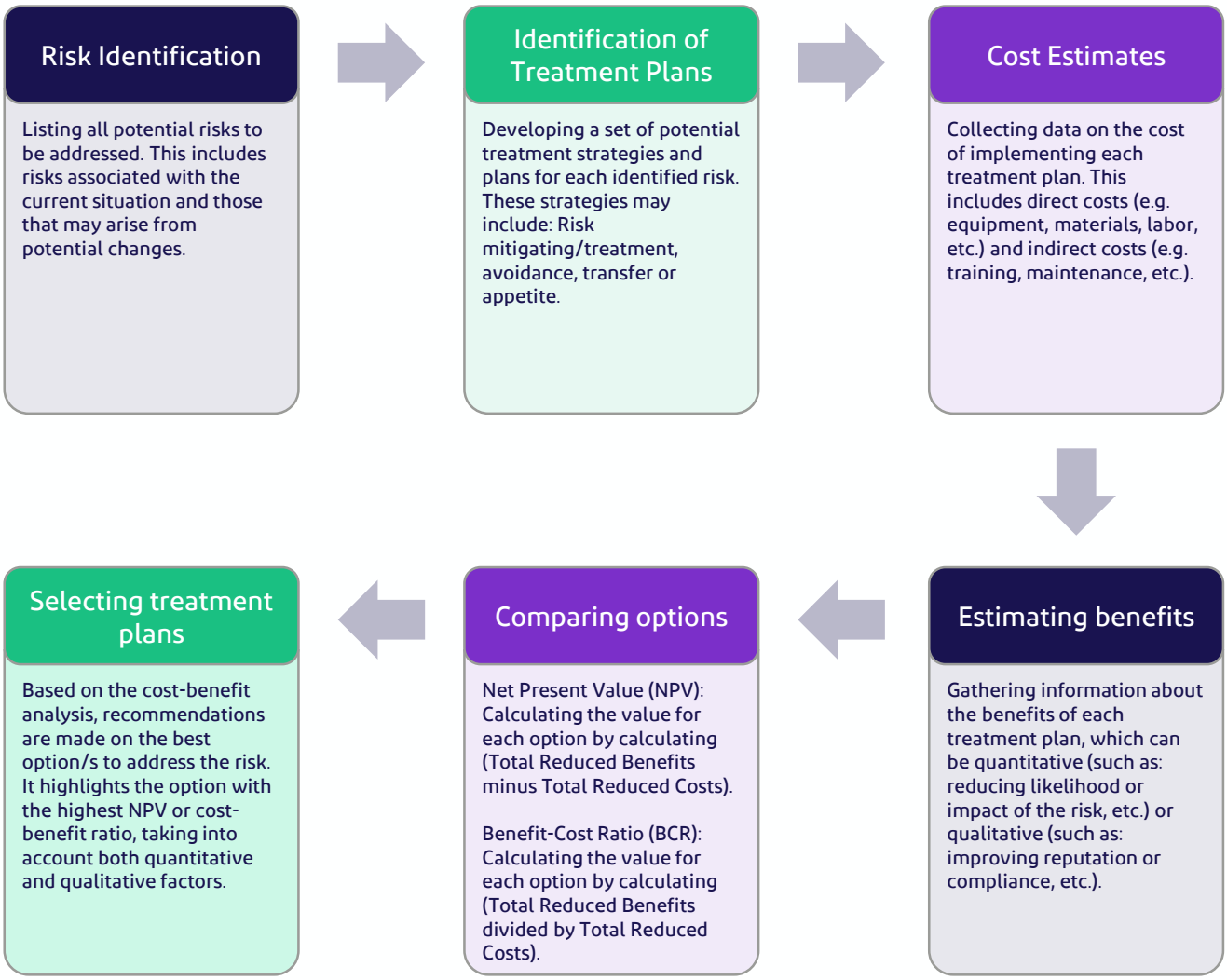


Figure (42): Benefit-Cost Analysis

[15]Referring to Reference No. (3) of Section (9). References and Sources.

5.1.5.2.3 Review, Follow-up and Communication

Periodic reviews of identified risks are conducted, along with monitoring the effectiveness of implemented controls and the progress of treatment plans. Continuous communication with risk owners within government entities is maintained to ensure the improvement of the quality and effectiveness of risk identification, assessment, treatment, and deliverables. Key or principle risks and key risk indicators (KRIs) are updated regularly to assist stakeholders and decision-makers in understanding the state of risks within the government entity and making appropriate decisions. The following is an explanation of the most prominent methods used to review, follow-up and communicate.

- Key components of review, follow-up and communication

Risk Register

Risks are recorded in the "Risk Register," a document that is regularly updated following each process of identifying, assessing, treating and reviewing risks. It serves as an official record of the risks identified, assessed and managed by the government entity responsible for risk management. This document aims to catalog all risks within the government entity and prepare reports that reflect all details of the identified risks. The following model (Table 20) illustrates the key fields for the processes of identifying, analyzing and treating risks:

Risk Identification						
Risk ID Code	Administrative Unit	Risk owner	Risk Description	Root Causes	Consequences of Risk	Classification of main risks and sub-risks
Risk Analysis and Assessment						
Inherent Impact	Inherent Likelihood	Inherent Risk Severity	Inherent Risk Severity	Applied Controls	Effectiveness of Controls	Residual Risk Severity
Risk Treatment						
Risk Treatment Strategy	Risk Treatment Plans	Owner of Treatment Plans	Targeted Implementation Date	Implementation Ratio	Status of Treatment Plans	Risk Treatment Strategy

Table (20): Risk Register Model

Risk Dashboard:

The risk dashboard serves as a centralized platform for analyzing and displaying the status of risks within the government entity. The importance of risk dashboards lies in their ability to facilitate direct monitoring and management of risks, thereby streamlining the process of generating risk reports and supporting decision-making. Table (21) below presents examples of risk dashboards, among others:

#	Dashboard	#	Dashboard
1	Inherent Risk Ratings Dashboard	5	Residual Risk Ratings Dashboard
2	Key Risks Rating Dashboard	6	Effectiveness of Applied Controls Dashboard
3	Inherent Risk Indicator Dashboard	7	Residual Risk Indicator Dashboard
4	Inherent Risk Heat Map Dashboard	8	Residual Risk Heat Map Dashboard

Table (21): Examples of Risk Dashboards

Figure (43) provides an illustrative example of Risk Dashboard Models16

[16] The above figure is an indicative model to illustrate the way the risk dashboard is displayed. The numbers mentioned do not reflect any real data or information.

- Risk Reports

Risk reports, shared with stakeholders, are among the most critical outputs of risk management. They provide an overview of risk levels and the support needed to mitigate negative impacts on the government entity.

The administrative unit responsible for the risk management system presents the results of risk identification, assessment and treatment to the committees overseeing risks and the stakeholders within the government entity. This ensures continuous and effective monitoring and follow-up of the treatment plans.

- Risk Governance Reports

Establishing standardized forms for risk reports to ensure comprehensiveness and support decision making by stakeholders. Risk reports include, but not limited to, the following:

- Risk Management System Report The report reviews the current status of the risk management system in the government entity, potential challenges, as well as the achievements of the administrative unit responsible for the risk management system, and others.
- Comprehensive Risks Status Report. The report reviews the status of all risks in the government entity. It includes the assessment of risk and controls applied, treatment plans, risk dashboards, etc.
- Detailed Risk Report: Risk management is tasked with preparing a detailed report, as needed. The report reviews a particular risk or risks, and accurately studies, analyzes and verifies them, proposing recommendations and solutions based on the results.
- Key or Principle Risk Report: The report reviews the status of the key/ principle risks in the government entity, in alignment with the views of senior management and stakeholders.
- Key Risk Indicators Report: The report reviews the status of key risk indicators (KRIs) with the aim of following up on potential risks and dealing with them proactively.
- Expected Risk Report: The report reviews the most important global and local risk statistics with the aim of supporting and enhancing proactivity in dealing with risks.
- Risk Radar Report: This type of report is tasked with highlighting emerging risks that may have a significant impact on the achievement of the organizational goals or priorities. Designs and charts are used in the development of a meaningful and impactful radar risk report.

- Risk Reports Frequency:
- Reporting frequency to stakeholders varies from one party to another, based on the directions of senior management and the Risk Steering Committee. Table (22) below provides an example of the reporting frequency model based on the risk severity [17]:

Reporting Frequency	Risk	Committee
Quarterly	Critical, High	• Risk Steering Committee. • Risk Committee emanating from the Board of Directors.
Last Committee Meeting of the Year	Critical, High, Moderate	
Quarterly/ Last Committee Meeting of the Year	• Key Risk Indicators (KRIs) • Key or Principle Risks	• Risk Steering Committee. • Risk Committee emanating from the Board of Directors.

Table (22): Reporting Frequency

[17] The above model is an indicative example only. Frequency and types of reports vary from one side to another depending on the nature of the business and the directions of stakeholders.

Supportive Tools for Review, Follow-up and Communication

- Risk Trend[18]

They are known as trends of change in the level or nature of the inherent or residual risk. They are used to follow up on the status of risks, changes to risks, and impact of risks on the government entity. The impact can positively or negatively impact the objectives of the government entity. A risk pattern or trend is influenced by a set of external factors, separately or jointly, such as: Emerging technologies, local regulatory and legislative changes, economic changes, and geopolitical incidents. Figure (44) below illustrates the risk trend model:

Figure (44): Risk Trend

- Key Deliverables of Activation Phase of Risk Management Processes

Figure (45) shows the most important deliverables of the activation phase of risk management processes:

Figure (45): Deliverables of Activation Phase of Risk Management Processes

5.1.5.3 Training and Improvement of Risk Management System

Risk management culture is a set of values, behaviors and common understanding about risks that are shared by all parties within the government entity. Training is a key component in enhancing the risk management culture of government entities, which will enhance the success of achieving risk management objectives by building the appropriate risk management culture for all parties involved (Figure 46).

[18]Referring to Reference No. (7) of Section (9). References and Sources.

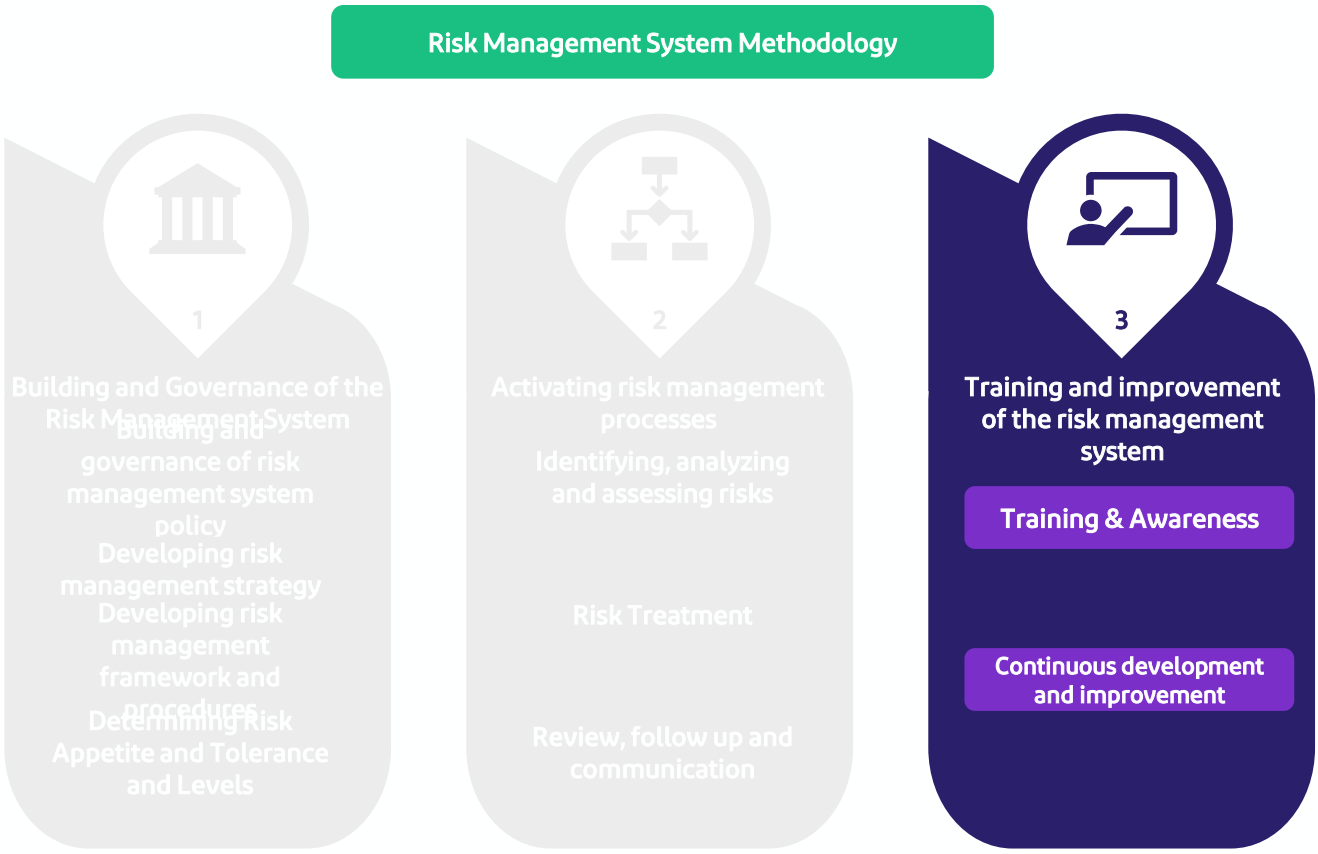


Figure (46): Training and Improvement of Risk Management System

5.1.5.3.1 Training & Awareness

The risk management team of the government entity shall cooperate with the administrative unit concerned with human resources in analyzing training needs to understand the training requirements of those involved in risk management. Further, they shall develop and implement a training plan for department's employees and Risk Champions commensurate with the roles and responsibilities stipulated in the risk management system of the government entity. The training program includes the required skills, such as: Technical skills, communication skills, teamwork, and strategic thinking.

An integrated program is also prepared to raise awareness of risk management at all organizational levels in the government entity, with the support of the senior management, through:

- Preparing and implementing training courses, and providing support to all units and departments concerned with providing appropriate information to conduct an assessment of the risks and controls.
- Holding workshops and brainstorming meetings within the government entity on a regular basis.
- Publishing awareness messages on the internal communication channels of the government entity.
- Identifying and planning an awareness day or week on risk management in the government entity.

- Identifying and providing digital training materials.
- Adopting more other activities to raise the levels of knowledge, awareness and readiness of the government entity's employees.

- Communication and Consultations

The processes and procedures of communication and consultation aim to support integration between the various administrative units and the administrative unit responsible for the risk management system within the government entity. Communication processes and procedures enhance ease exchange of information and ensure its accuracy and integrity.

The communication mechanisms in government entities vary depending on the nature of the entity's operations and the approved organizational structure. The administrative unit responsible for the risk management system within the government entity must develop clear mechanisms and establish unified communication and consultation channels, including, but not limited to, the following:

- Creating a communication channel via the email.
- Creating a communication channel through the internal portal of the entity.

- Risk management Culture

A risk culture is a key factor that affects the government entity's risk management system. Promoting a risk culture within the government entity enhances the adoption of a risk-based approach and integrates risk management into the daily tasks and operations of employees, under the leadership and support of the senior management of the government entity.

Factors Enhancing Risk Management Culture in the Government Entity:

- Senior management's interest and participation in adopting a risk-based approach.
- Creating a flexible environment that encourages government entity's employees to freely communicate and discuss current and emerging risks.
- Integrating risk management practices into performance assessment and reward systems, and encouraging individuals to fulfill their roles in risk management.
- Sharing and promoting success stories, making them examples to be followed in risk management practices.

- Developing and implementing comprehensive training programs to raise awareness of the risk management system and providing sufficient resources for effective risk management, including the necessary technological tools.
- Adopting the enhancement of the ability to identify, analyze, and assess current risks, as well as anticipate and infer emerging risks that may affect the achievement of strategic objectives among the government entity's employees.

5.1.5.3.2 Continuous Development and Improvement

The documents of the risk management system are reviewed periodically according to the approved review mechanism for each document, or when a significant change occurs in the work environment or the strategic or operational objectives of the government entity.

The effectiveness of the risk management framework and procedures is monitored by evaluating the maturity level of the risk management system in the government entity, comparing it with global and local standards, and developing a strategy to improve the performance of risk management. It is important for the government entity to assess the maturity level of risk management periodically, taking into account aspects of governance and culture, the risk management strategy and its alignment with external trends, the government entity’s strategy, the effectiveness of risk identification and assessment, and the effectiveness of risks follow-up and control, using one of the following review methods:

- Self-assessment
- Assessment of Risk Management KPIs.
- Internal or external audit, using auditing methods and programs approved internally, or by an external independent party

Self-Assessment of Risk Management System

The maturity level of the risk management system is evaluated periodically by the administrative unit responsible for the risk management system based on the risk management and business continuity controls of the digital government issued by the Digital Government Authority and other local legislation and regulations. Figure (47) provides a model for assessing the maturity level, which is based on the axes of governance, management, policies and procedures, and development:

Level 1 (Emerging)	Level 2 (Developed)	Level 3 (Established)	Level 4 (Advanced)	Level **5** (Exceptional)
Policies and Procedures: There are no policies and procedures for the risk management system.	**Policies and Procedures:** There is an initial documentation of unified policies and procedures for the risk management system.	**Policies and Procedures:** Risk management policies and procedures are documented and approved.	**Policies and Procedures:** Risk management policies and procedures are part of the government entity's culture.	**Policies and Procedures:** Providing the efforts required to improve and develop the risk management policies and procedures.
Development: There are no unified standards for development.	**Development:** There are standards for development, but they are not necessarily linked to the objectives of the government agency.	**Development:** The bases of the risk management system are completely developed.	**Development:** Risk management practices are integrated into strategic planning of the government entity.	**Development:** Risk management is developed based on unified standards and improvement indicators, with the use of technological tools and business automation.
Management: Senior management's awareness of risk management system practices is limited.	**Management:** Senior management is aware of the risk management system practices, but has no input into the decision-making process.	**Management:** Senior management is aware of and supports risk management processes at the government entity's level.	**Management:** Senior management is directly involved in defining the risk appetite framework.	**Management:** There is direct support from senior management to improve risk management practices and processes.
Governance: There is little communication, and risks are dealt with interactively without prior planning.	**Governance:** A risk management system is considered during performance assessment. There is a general understanding in most areas of the business of the risk assessment role.	**Governance:** There is a standardization, coordination and enhancement of the risk management system of all business units. Risks are taken into account during the implementation of business and allocation of resources.	**Governance:** There is clear governance for all RMS processes and a clear understanding of roles and responsibilities.	**Governance:** The risk management system is integrated. A risk-based approach is applied in the decision-making process.

Figure (47): Model of Assessing Risk Management Maturity Level

Assessment of Key Performance Indicators

Key performance indicators (KPIs) are an important measurement tool that helps the government entity assess the effectiveness of the risk management system implementation. KPIs for the risk management system and their target values are determined in alignment with strategic and operational goals, as well as the objectives of the administrative unit responsible for the risk management system in the government entity. KPIs are reviewed periodically to ensure efficiency and improve performance levels. Table (23) below provides an example of KPIs Model:

#	Key Performance Indicator	Targeted Value for the Year	Review Frequency
1	(%) of risks occurred and not covered or recorded in the register.	X%	Yearly
2	(%) of risks for which treatment plans were not implemented on time.	X%	Yearly
3	(%) of compliance with the relevant internal requirements in the government entity.	X%	Yearly
4	(#) of awareness campaigns on the risk management system for the government entity's employees.	X	Yearly
5	(#) of reports submitted to the relevant committees and stakeholders.	X	Yearly
6	(%) of achieving the objectives of the administrative unit responsible for the risk management system in the government entity.	X%	Yearly
7	(%) of implementation of the annual risk assessment plan for the administrative units in the government entity.	X%	Yearly
8	(%) of achieving the targeted percentage of compliance with local legislation and regulations related to the risk management system.	X%	Yearly

Table (23): KRIs Model

Key Deliverables of Training and Improvement Phase

Figure (48) shows the most important deliverables of the training and improvement phase.

Figure (48): Key Deliverables of the Training and Improvement Phase

Key deliverables of the risk management system methodology phases

Figure (49) outlines all key deliverables related to the risk management system in the government entity:

Figure (49): Key Deliverables of the Risk Management System

- Implementation of the risk management system's methodology in the government entity

The government entity is studying the current status in risk management and the management maturity level to apply the risk management methodology, thereby contributing to raising the maturity levels of risk management within the government entity. Below are examples of some key cases of risk management maturity levels:

- Case 1 – Absence of a dedicated administrative unit for risk management within the government entity.

In the absence of a dedicated administrative unit for risk management within the government entity, it is recommended to establish the risk management structure, develop its policies, procedures, and strategy, and then begin risk assessment and mitigation processes, along with training and improvement, as outlined in the methodology (Figure 50).

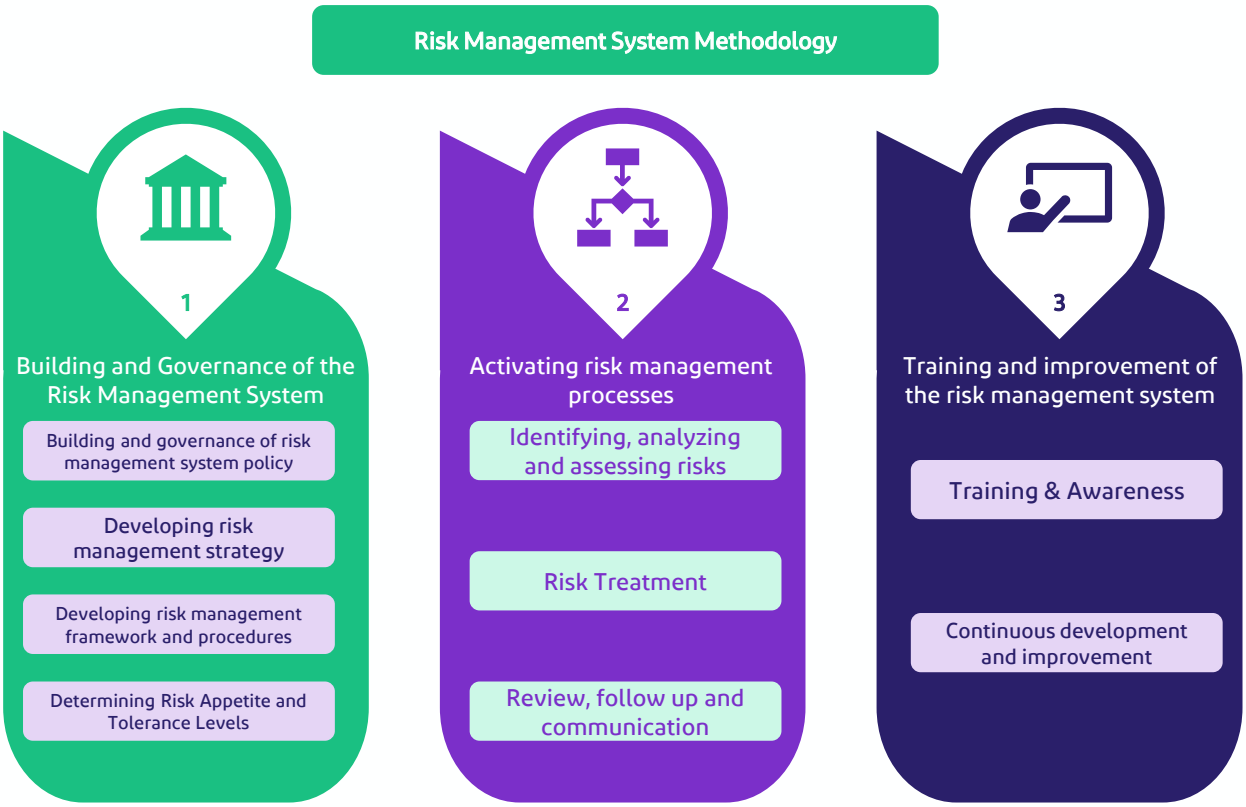


Figure 50 - Risk Management System Methodology

Case 2 – Existence of a risk management department, activities or procedures within the government entity

If a risk management department exists, or if there are certain risk-related activities or procedures within the government entity, it is recommended to assess the current status of risk management to identify gaps compared to the risk management methodology outlined in the Digital Government Authority's Risk Management and Business Continuity Controls for Digital Government. Based on this assessment, a work plan should be developed to enhance and improve risk management, as illustrated in the methodology (Figure 51)

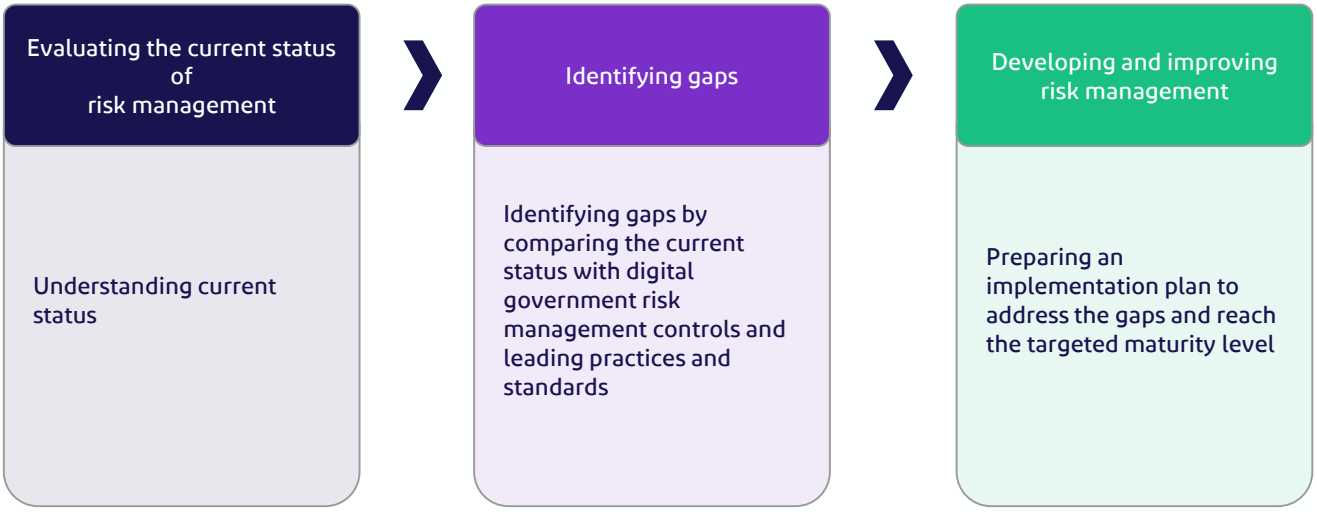


Figure (51): Risk Management System Development Methodology

5.2

Business Continuity Management System

5.2.1 Significance of Business Continuity Management System

The Business Continuity Management System primarily focuses on ensuring the sustainability of the businesses and services of the government entity and enhancing its ability to recover key operations and services amidst risks and disasters. This is achieved through the use of specific resources and technologies within a defined time frame. Figure (52) outlines the key benefits and main deliverables of implementing the business continuity management system in the government entity.

Figure (52): Most Important Benefits of the Business Continuity Management System

1. Enhancing the resilience and sustainability of key businesses and services in the government entity

Ensuring the ability of the government entity to continue to provide key services efficiently during times of disruption, and facilitating recovery and return to normalcy procedures. This maintains the stability of the government entity and supports its long-term growth.

2. Minimizing the impact of disruptions

Mitigating the impact of crises and disasters on the operations and services of the government entity by planning for potential disruptions and implementing preventive measures, which include: Minimizing downtime and associated costs.

3. Raising the ability to make decisions in times of crisis

Effective business continuity planning provides a clear framework and set of protocols for decision-making during a crisis, which significantly reduces the time taken to make critical decisions and ensures a rapid and effective response to minimize the impact of disruption.

4. Enhancing the culture of the government entity and the confidence of stakeholders

Demonstrating the ability and commitment of the government entity to maintain the provision of services in times of crises and disasters contributes to building trust among all stakeholders, including beneficiaries, suppliers and investors. It also contributes to enhancing the reputation of the government entity.

5. Supporting the Realization of Strategic Objectives

Identifying threats that may affect the realization of the strategic objectives of the government entity, and developing plans and initiatives to address and deal with them.

5.2.2 Principles of the Business Continuity Management System

To develop an effective and successful business continuity management system, it is necessary to understand the objectives of the government entity and the flow of operations. It is also necessary to determine the strategic and operational objectives of the business continuity management system, and the system's scope of work. Alongside understanding the needs and expectations of stakeholders and concerned parties, the process involves identifying business commitments, internal and external dependencies, suppliers, and service providers. It also includes establishing and developing a business continuity policy, defining authorities, roles, and responsibilities, and determining the competencies, resources, and effective methods to support the implementation of the Business Continuity Management System. This is followed by conducting a business impact analysis, risk assessment, and developing strategies and plans for response, recovery, and restoration of operations across different categories. Subsequently, monitoring, reviewing, verifying, auditing, and performance assessment processes are carried out. Finally, continuous development and improvement processes are implemented as shown in Figure (53).

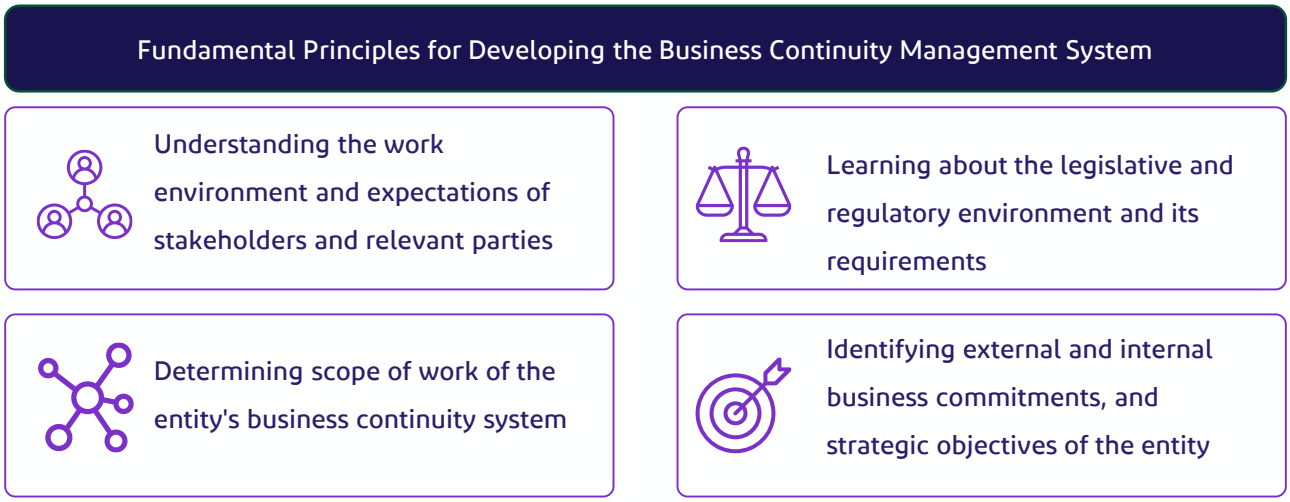


Figure (53): Fundamental Principles for Developing the Business Continuity Management System

5.2.3 Success Factors of the Business Continuity Management System

The successful implementation of the of the business continuity management system of the government entity depends on a set of factors, most prominently:

- Including the business continuity management system as a key component of the decision-making process.
- Support and interest of leaders and senior management in implementing the requirements of the business continuity management system.
- Enabling the administrative unit responsible for the business continuity management system, thereby raising the performance level of the government entity, as necessary for business and digital services continuity.
- Monitoring the effectiveness of tasks and activities within the business continuity management system, while adhering to and implementing international standards, best practices, and relevant regulatory requirements.
- Ensuring the commitment of stakeholders at all levels to perform their assigned tasks and implement all business continuity plans and strategies.
- Automating processes related to the business continuity management system to ensure efficiency and enable the continuous generation of relevant reports.
- Aligning with external entities, suppliers, and service providers.
- Continuous improvement through learning from successful experiences, exercises, and best practices in the field.

5.2.3.1 Key Success Factors for a Business Continuity Management System

Governance is the mechanism through which the business continuity management system is managed within the governmental entity. It encompasses a set of rules, regulations, standards, and procedures that define the roles, responsibilities, and relationships among all parties to achieve excellence in performance and make appropriate decisions. The key elements include:

- Understanding the governmental entity's scope of work and responsibilities.
- Defining the authorities and responsibilities of stakeholders and relevant parties, as well as their needs and expectations.
- Determining the scope and objectives of the business continuity management system, in alignment with the objectives of the governmental entity.

- Identifying and developing key performance indicators that align with the entity's functions and objectives.
- Identifying the requirements of the business continuity management system that support its implementation and sustainability.
- Determining the frequency of reporting and communication among relevant stakeholders.

5.2.2.4 Standards of the Business Continuity Management System

There are various international standards, local regulations, frameworks, principles, and guidelines for the business continuity management system that assist in building and activating the system by applying best practices with high efficiency. Among the most important local standards used in developing and implementing the business continuity management system: The Risk Management and Business Continuity Controls for Digital Government issued by the Digital Government Authority. The National Framework for Risk, Emergency, and Business Continuity Management issued by the General Secretariat of the National Risk Council. On the international level, the most prominent standards include those issued by the International Organization for Standardization (ISO), such as: International Business Continuity Management Standard (ISO 22301:2019), Business Continuity Guidelines (ISO 22330:2018), Business Impact Analysis Guidelines (ISO 22317:2015), and Business Continuity Management Exercise Guidelines.(ISO 22398:2013)

5.2.5 Methodology of the Business Continuity Management System

The methodology of the business continuity management system has been prepared in line with the Plan-Do-Check-Act methodology, as shown in Figure (54) below. It aims to support compliance with the risk management and business continuity controls for digital government issued by the Digital Government Authority.

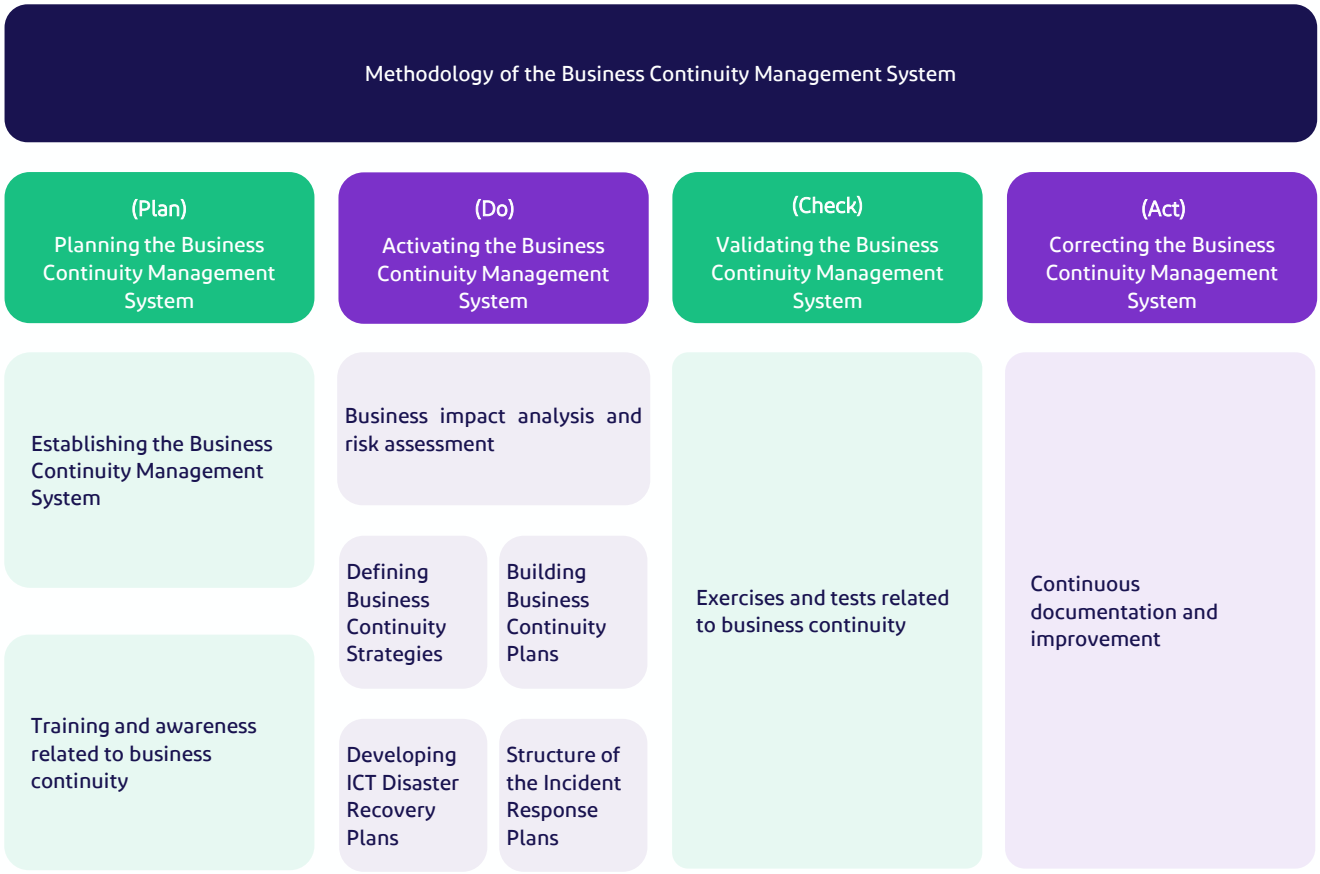


Figure (54): Methodology of the Business Continuity Management System

5.2.5.1 Planning the Business Continuity Management System

The planning of the Business Continuity Management System involves understanding the context of the government entity's operations and Business Continuity Management System's scope, based on the internal and external requirements related to the entity's goals and strategic vision. It aims to develop the business continuity policy and strategies, clarify its objectives, controls, procedures, and the roles and responsibilities of stakeholders. The outcomes of this planning process support and enhance the government entity’s policies and objectives. Additionally, the planning includes developing the Business Continuity Management System's objectives to align with the government entity's strategy. This process incorporates the entity's organizational context and scope, ensuring they are shared with stakeholders and relevant parties.

5.2.5.1.1 Establishing the Business Continuity Management System

The Organizational Structure of the Business Continuity Management System – in Case There is a Board of Directors for the Government Entity (Form 1):

Figure (55) shows a model of the organizational structure in the case there is a board of directors for the entity. It includes the business continuity committee emanating from the board of directors, the steering committee, and the administrative unit responsible for the business continuity system.

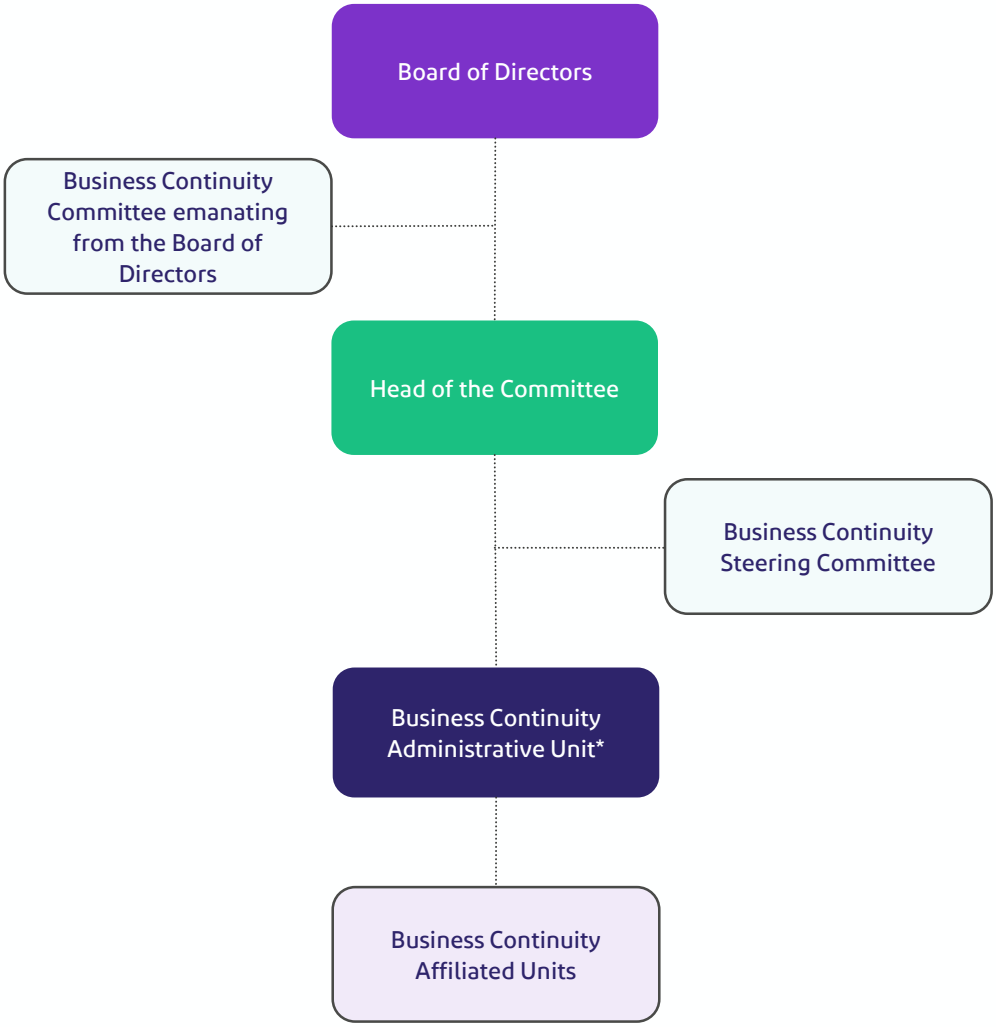


Figure (55): Illustrative Example of Form 1 - Organizational Structure of the Business Continuity Management System

The Organizational Structure of the Business Continuity Management System – in Case There is no Board of Directors for the Government Entity (Form 2):

Figure (56) shows a model of the organizational structure in the case there is no board of directors for the entity. It includes the steering committee and the administrative unit responsible for the business continuity management system.

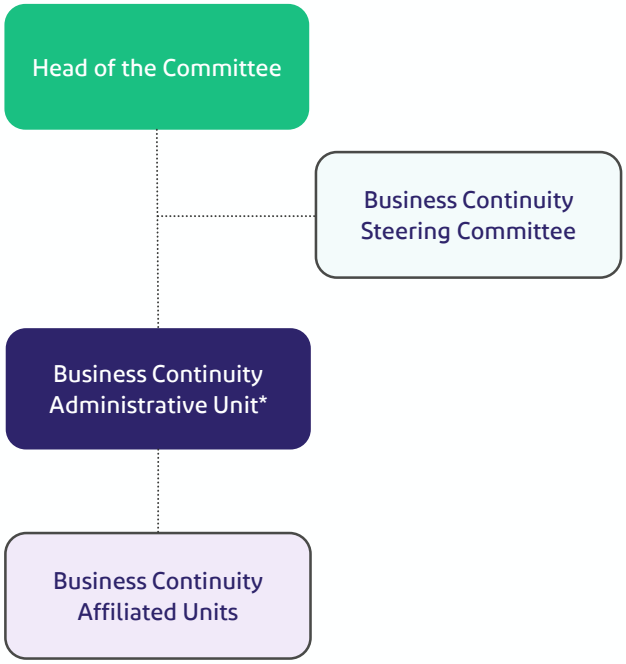


Figure (56): Illustrative Example of Form 2 - Organizational Structure of the Business Continuity Management System

Roles and Responsibilities[19]

Roles and responsibilities within Business Continuity Management are established and defined to contribute to achieving better outcomes, such as saving time and costs, increasing efficiency, and enhancing transparency and accountability among stakeholders.. Below are the key responsibilities of stakeholders and relevant parties involved in implementing the Business Continuity Management System.

1. Board of Directors[20]

- Supervising the business continuity management system and fostering a business continuity culture within the government entity.
- Ensuring, supporting and guiding the independence of the administrative unit responsible for the Business Continuity management System, in accordance with the organizational structure of the government entity. Additionally, ensuring the availability of sufficient financial and human resources to support the implementation and execution of the Business Continuity Management System operations.

[19]The above roles and responsibilities are only indicative examples, and the roles and responsibilities vary from one side to the other depending on the nature of the business.

[20]If the government entity does not have a Board of Directors, the authority is delegated to the Chief Executive of the entity.

- Guaranteeing clarity of roles and responsibilities related to the Business Continuity Management System to support effective governance and enhance decision-making across all executive, administrative and operational levels.
- Adopting a business continuity management strategy, policy and framework.

2. Business Continuity Committee emanating from the Board of Directors (if any)[21]

- Reviewing the analysis reports of business interruption impact periodically or as needed in the event of significant changes within the government entity.
- Considering and reviewing the strategies and plans taken by the government entity for business continuity and disaster recovery.
- Review and recommend the adoption of business continuity and disaster recovery policy, strategies, and plans, prior to its approval by the Board of Directors.
- Reviewing annual reports from internal and external auditors on the implementation of the Business Continuity Management System's policies and procedures within the government entity, and providing recommendations and support for system improvements, as needed.

3. The Chief Executive in the Government Entity/ Authorized Person

The Chief Executive/ Authorized Person in the government entity shall be responsible for supervising the business continuity management system. Further, he bears the general responsibility, which includes approving the policy and appointing an official to implement the business continuity management system.

4. Steering or Supervisory Committee of the Business Continuity Management System

The existence of a steering or supervisory committee for the business continuity management system aims to follow-up and supervise the implementation of the system, and provide the necessary support to achieve the strategic objectives. Its most important responsibilities include:

- Supervising the implementation and effectiveness of the business continuity management system.
- Reviewing the business continuity policy and providing feedbacks.
- Approving the Business Continuity Management Framework.
- Approving the business impact analysis results.
- Approving the timeframe for recovery of operations, and identifying risks that require treatment.

- Approving the timeframe for recovery of operations, and identifying risks that require treatment.
- Implementing the initiatives plan, monitoring business continuity objectives, and studying and approving the proposed changes.
- Approving the annual training system and awareness-raising programs.
- Reviewing post-incident or exercise reports, and taking the necessary decisions thereon.

3. Party responsible for the Business Continuity Management System

- Ensuring the implementation of the Business Continuity Management System's policy, strategy and framework, and ensuring that the necessary resources are provided to implement the requirements of the system.
- Overseeing the analysis and evaluation of the Business Continuity Management System's requirements and priorities, and identifying key objectives and indicators.
- Designing, implementing and managing business continuity and disaster recovery plans, strategies and procedures.
- Coordinating, organizing and sharing periodic tests and exercises of the business continuity plans, evaluating their results, and identifying areas for improvement and development.
- Continuously monitoring, evaluating and updating the Business Continuity Management System, in accordance with internal and external changes and risks.
- Participating in awareness-raising activities on the importance of business continuity, such as exercises and training workshops.
- Collaborating and coordinating with the relevant internal and external entities to ensure the implementation of the business continuity management system's practices.
- Representing the unit responsible for business continuity management in periodic reviews and evaluations of the system.

3. Party responsible for the Business Continuity Management System

- Developing, implementing, reviewing and publishing the latest versions of the Business Continuity Policy and Framework.
- Preparing the initiative plan and the annual objectives of the business continuity system.
- Conducting risk assessment and interruption impact analysis workshops.
- Developing and reviewing the business continuity strategy, in cooperation with the various administrative units within the government entity.

- Developing and reviewing the business continuity plans in cooperation with various administrative units within the government entity.
- Following-up on the implementation of corrective actions to address incidents.
- Developing the annual training program to ensure the effectiveness of the roles of the responsible teams involved.

7. Champions of the Business Continuity Management System

Business continuity champions are considered one of the most important basics of the system, where a representative is nominated from each administrative unit within the government entity, within the scope of their competencies. Most important responsibilities of the business continuity champions include: Representing administrative units, participating in risk identification and analysis, analyzing the impact of business interruption, determining target recovery times and points, contributing to the development of preventive plans and actions, and implementing the corrective actions.

8. Administrative Unit responsible for Information and Communication Technology (ICT)

- Developing, updating and activating ICT disaster recovery strategies and plans.
- Participating in risk assessment workshops and interruption impact analysis workshops.
- Ensuring the implementation of technological solutions for business recovery and remote working.
- Implementing tests for ICT disaster recovery plans, in alignment with the administrative unit responsible for the business continuity management system and relevant departments.

9. Administrative Unit responsible for Cybersecurity

- Analyzing and assessing cyber risks, and identifying preventive and precautionary measures to mitigate these risks.
- Designing, implementing and testing cyberseurity and disaster recovery plans and strategies.
- Developing and updating cyber incidents response plans.
- Participating in risk assessment workshops and interruption impact analysis workshops.
- Participating and providing the necessary support in implementing the relevant tests.

10. Administrative Unit responsible for Human Resources

- Identifying, analyzing and evaluating activities, risks and associated human resources, and identifying their respective needs, expectations and responsibilities.
- Developing, implementing and reviewing the BCMS's policy, plans, programs and procedures associated with human resources.
- Participating in risk assessment workshops and interruption impact analysis workshops.
- Participating and providing the necessary support in implementing the relevant tests.

11. Administrative Unit responsible for Safety, Security and Facilities

- Participating in risk assessment workshops and interruption impact analysis workshops.
- Designing, implementing and testing security and emergency plans for buildings and facilities.
- Participating and providing the necessary support in implementing the relevant tests.

12. Administrative Unit responsible for Service Providers and Suppliers

Service providers should be required to ensure that all personnel involved in outsourcing services, including subcontracting, are aware of their responsibilities towards the Business Continuity Management System. Responsibilities and obligations should be formally included in contracts relating to business continuity plans. The following are the most important responsibilities of the unit:

- Ensuring that the performance of suppliers and service providers is classified according to service level agreements.
- Ensuring the existence of a business continuity system for external parties contracting with the government entity.
- Ensuring that relevant suppliers or service providers participate in the plans tests at the government entity (if required).
- Participating and providing the necessary support in implementing the relevant tests.

13. Administrative Unit responsible for Internal Audit/ Review

- Carrying out audits, test controls, standards and practices, and identifying non-conformities and opportunities to ensure compliance with the relevant national legislations.
- Auditing the business continuity management system in line with international standards, such as (ISO 22301)
- Presenting BCMS audit reports to stakeholders.
- Conducting audit follow-up activities, ensuring the implementation of corrective plans, and assessing their effectiveness.

14. Administrative unit managers in the government entity:

- Ensuring the implementation of the business continuity policy and framework, and ensuring that tasks are carried out within the departments, and necessary resources are provided.
- Nominating business continuity champions from the relevant department.
- Providing support, time, and resources to business continuity champions.
- Participating in building and updating related business continuity plans.
- Participating and providing the necessary support in implementing the relevant tests.
- Participating in risk assessment workshops and interruption impact analysis workshops.

15. All administrative units in the government entity

- Participating in risk assessment workshops and interruption impact analysis workshops.
- Participating in the development and design of business continuity plan testing exercises.
- Participating and providing the necessary support in conducting tests for the relevant business continuity plans

Policy of the Business Continuity Management System

The business continuity management system policy is developed and documented within the government entity to enhance leadership and administrative direction. This aims to support the system as part of the governance of the business continuity management system. The system's objectives and scope, and stakeholders' roles, responsibilities, along with the policy items are defined and shared with all employees of the government entity, and are applied throughout the entire entity.

Objectives of the Business Continuity Management System

The objectives of implementing the business continuity management system, along with its controls, processes and procedures are determined while considering what the system aims to achieve, the required resources, and party responsible in this respect. Some of the key goals for implementing the business continuity management system include:

- Protecting the entity's reputation: The government entity's ability to demonstrate to beneficiaries and stakeholders that it is prepared to face a crisis or disaster and can recover quickly. Comprehensive business continuity planning indicates that the entity has the flexibility to handle even significant disruptions.
- Reducing financial losses: Reducing the losses that could be caused by a crisis or disaster, as the government entity will be able to resume operations more quickly.
- The government entity relies on the technological and digital infrastructure to ensure its operations continue during disruptions. This is vital for maintaining stability and delivering essential services to beneficiaries.

Organizational Scope of Work:

The scope aims to define the boundaries of the business continuity system and its applicability, to ensure the government entity's ability to cover all services, activities, locations, resources, suppliers, service providers, stakeholders, and relevant parties. The context also includes understanding the needs and expectations of stakeholders, as well as the objectives and commitments of the government entity. It is important to prepare a document that defines the scope of the Business Continuity Management System with a methodology that suits the size of the government entity and the nature of its activities, and to ensure that this document is made available to all relevant parties. Figure (57) provides an illustrative example of the general organizational scope for business continuity.

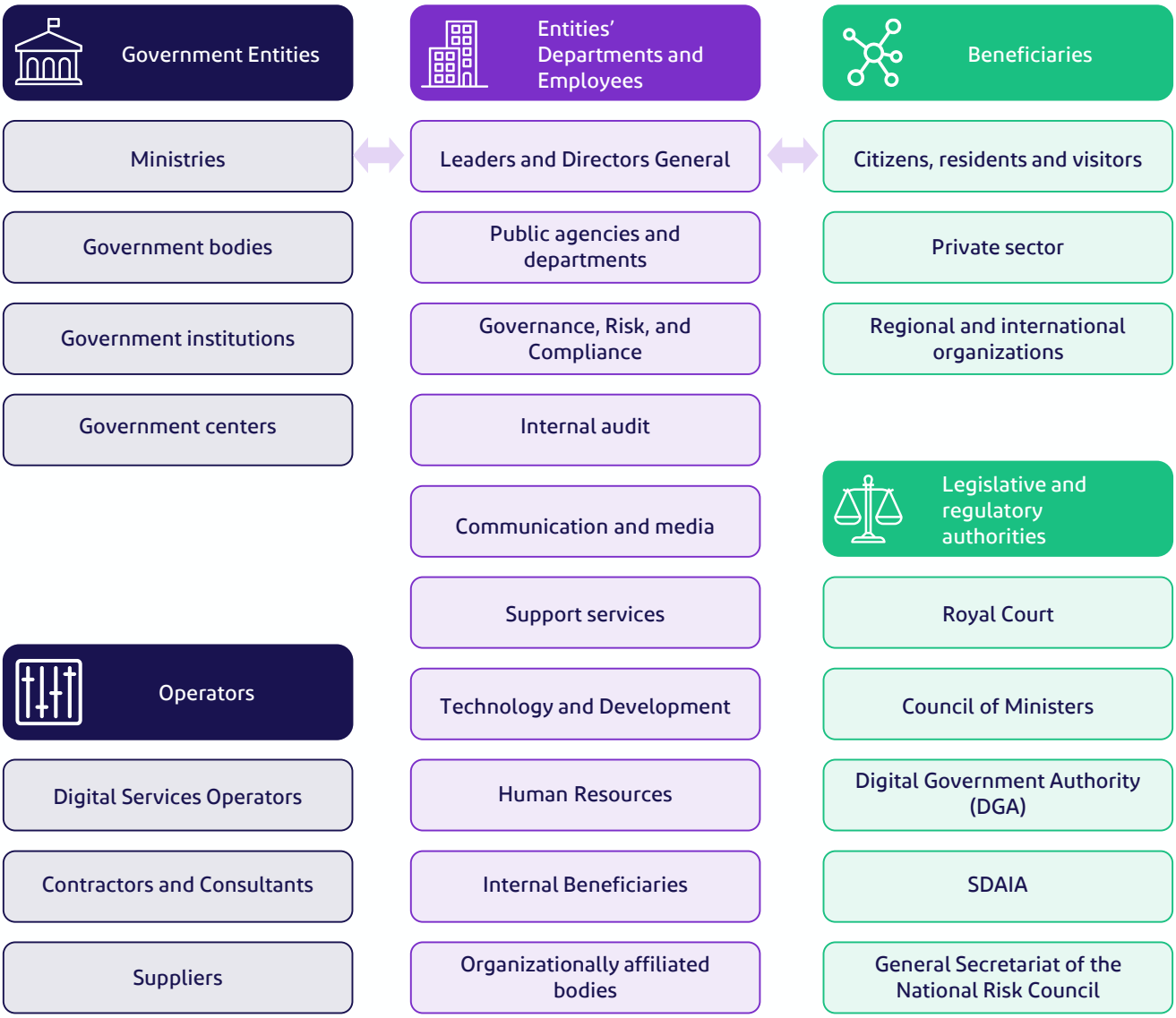


Figure (57): Illustrative Example of the General Organizational Scope of Business Continuity

Framework and Procedures for the Business Continuity System

Planning the Business Continuity Management System

The alignment between the business continuity policy, objectives and processes is clarified, ensuring consistency with the policies and goals of the government entity. This phase focuses primarily on developing the Business Continuity Management Framework through:

- Identifying the requirements and scope of business continuity management by assessing the overall situation, including: Activities of the government entity and stakeholders' requirements
- Identifying risks and opportunities in line with the business continuity management system, and developing comprehensive action plans until creating business continuity plans.
- Creating the necessary activities and processes to operate the Business Continuity Management System.

Documenting and approving the Business Continuity Management System documentation

- The policies, standards, and supporting information for business continuity are documented, presented, and approved by the key stakeholders according to the entity' approved authority matrix. Continuous awareness is ensured, and shall be made available to all stakeholders, when needed.

5.2.5.1.2 Training and Awareness of the Business Continuity Management System

Efforts are made to develop and document annual training plans to raise awareness of the Business Continuity Management System across the government entity, in collaboration with relevant departments. Implementing the training and awareness program requires a set of activities, including, but not limited to:

- Defining the objectives and expected deliverables of the training and awareness activities.
- Identifying the targeted groups and the appropriate level for each group.

- Identifying the available resources and means for training and awareness.
- Designing the content, methodology, and training and awareness approaches.
- Implementing the training and awareness programs and activities on a regular and organized basis.
- Evaluating the results, impacts, and the required improvements.

Additionally, the awareness activities include implementing and disseminating awareness campaigns about the Business Continuity Management System. Some of the dissemination methods and channels include, for example:

- Open discussion meetings and sessions
- Workshops
- The entity's internal website (internal digital portal)
- Business Continuity Awareness Week
- Awareness messages
- Newsletters
- Awareness banners
- Email

In collaboration with the Human Resources Department, staff training on multiple skills and succession planning can be integrated, as outlined in the appendices.

5.2.5.2 Business Continuity Management System Activation Phase

Based on the deliverables of the planning phase, the activation phase begins, during which the following actions are undertaken:

- Analyzing the impact of disruptions on operations and procedures that deliver products and services, and determining the target recovery time for key services following a disruption.
- Identifying and evaluating internal and external risks and threats, as well as critical failure points that may affect priority activities. Assessing their expected impact in the event of a disruption or disturbance and devising solutions to address or mitigate their effects.
- Defining and documenting the procedures based on the deliverables of the selected strategies and solutions.
- Developing Business Continuity Plans
- Specifying the structure of incident response plans, the mechanism for activating business continuity plans, and internal and external communication strategies.
- Developing and documenting ICT Disaster Recovery Plans to ensure the government entity's ability to respond to crises, disruptions, or emergencies affecting information systems, communications, and digital services.

5.2.5.2.1 Business Interruption Analysis (BIA)

Business Interruption Analysis is conducted by analyzing business activities and assessing the impacts of their disruption. This process aims to identify strategies to be implemented in the event of interruptions, disturbances or incidents Determining the priority of procedures and activities based on their importance in providing products and services. The BIA phase is considered the main driver for business continuity and ensuring the effectiveness of plans. This phase is executed by identifying all internal and external procedures and operations of the entity, specifying the procedures they rely on, and analyzing the impact of interruption over time based on the approved interruption impact assessment matrix of the entity, while clarifying the entity's critical operations or procedures.

Upon completing the Business Interruption Analysis, the entity identifies and classifies critical procedures, evaluates and determines their recovery times, including the targeted recovery time (RTO), the targeted recovery point (RPO), the maximum tolerable period of disruption (MTPD), the minimum business continuity objectives (MBCO), and the resources required to recover operations, such as: Human resources, equipment, technological systems, and facilities.

The timeline for the business disruption impact is determined based on the sensitivity of the government entity's operations and services. For example, some entities consider that the impact of disruption on certain operations begins after half an hour due to their sensitivity. Therefore, it is preferable for the timeline of disruption impact to start from half an hour. In other cases, the impact may begin after a day or two, so the timeline for impact assessment starts accordingly from a day or two. Figure (58) outlines the difference between the targeted recovery time (RTO), the targeted recovery point (RPO), and the maximum tolerable period of disruption (MTPD).

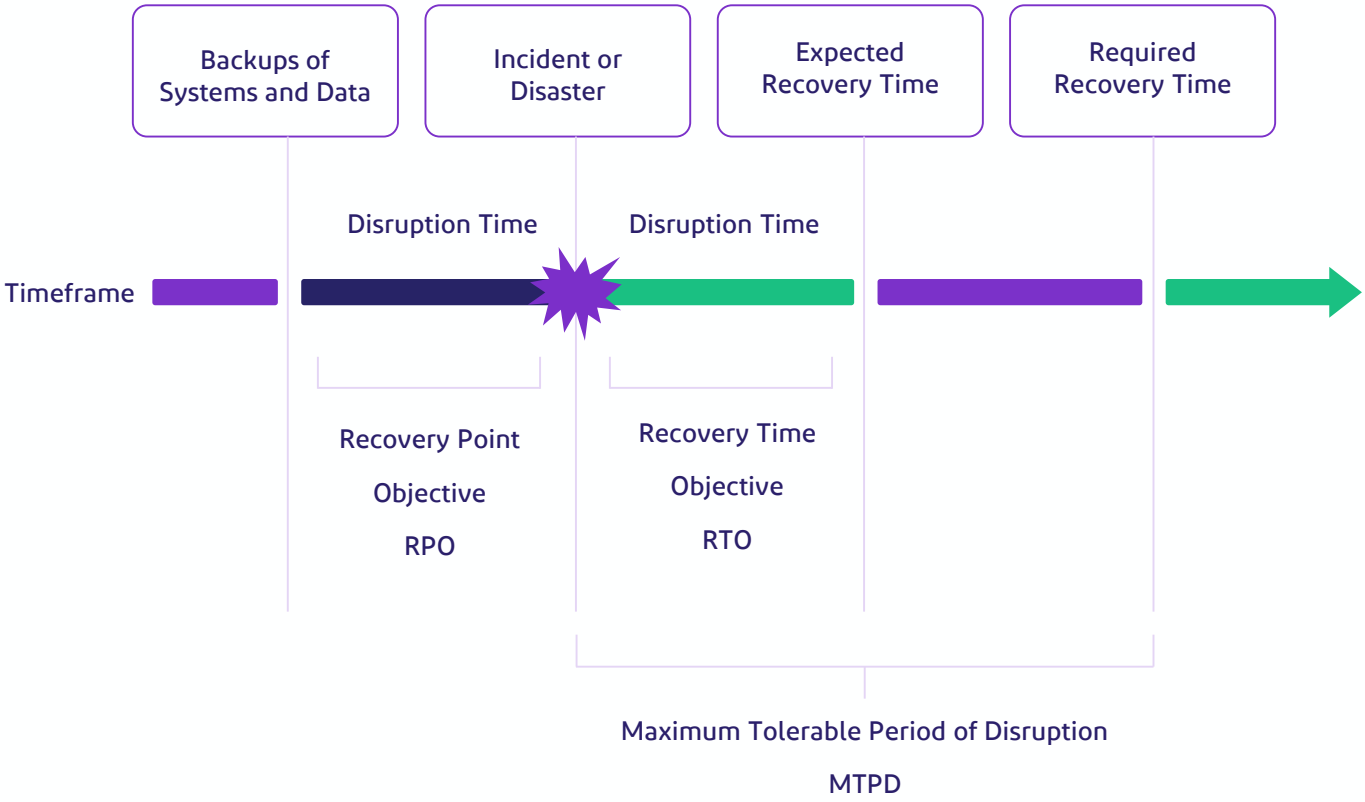


Figure (58): Example of Recovery Times

Classification of Government Platforms and Applications and Defining Their Targeted Recovery Times

To organize the digital government's operations and achieve its objectives across various aspects, the Authority has developed a matrix for classifying government platforms and applications (Figure 59). Each entity is expected to classify its platforms for different beneficiaries based on this matrix, adopting the highest level of impact in cases where the levels of impact vary among factors. Accordingly, entities can begin working on setting the targeted recovery time for each level as outlined in the figure, thereby supporting the continuity of digital government's services at each respective level.

Analysis of Impact Level	(Stakeholder Impact)	(Financial Impact)	(Legal and Regulatory Impact)	(Reputational Impact)	Targeted Recovery Time **RTO
Very Critical	Complete impact on the digital platforms and applications provided across Saudi Arabia, affecting all of the following beneficiaries. Government Entities Businesses and Supply Chains Citizens and Residents	Financial losses of up to SAR 1,000,000 per hour or 0.0115% of the total annual revenues generated by this service, whichever is greater.	Results in the loss of compliance certification (local/international) or exposure to lawsuits and penalties from local authorities or international courts due to breach of local or international laws.	Causes damage and negative impact on the overall reputation of the digital government in local and/or international media, leading to a decline in the Kingdom's ranking on the United Nations E-Government Development Index.	4 Hours
Critical	Complete impact on the digital platforms and applications provided across Saudi Arabia, to include on or more of the following beneficiaries Government Entities Businesses and Supply Chains Citizens and Residents	Financial losses of up to SAR 500.000 per hour or 0.00575% of the total annual revenues generated by this service, whichever is greater.	Results in the suspension of compliance certification (local/international) or exposure to lawsuits and penalties from local authorities due to legal violations.	Causes damage and negative impact on the entity's reputation in local and/or international media.	8 Hours

Important	Complete impact on the digital platforms and applications provided across one or more regions of Saudi Arabia, affecting one of the following beneficiaries within these regions. Government Entities Businesses and Supply Chains Citizens and Residents	Financial losses of up to SAR 100,000 per hour, or 0.00115% of the total annual revenue generated by this service, whichever is greater.	Leads to a warning notice for the suspension of compliance certification, along with a request for clarification of the incident and immediate treatment from regulatory bodies, or the potential for legal accountability from relevant authorities.	Causes a limited negative impact on the entity's reputation in local media and complaints from beneficiaries.	12 Hours
Moderate	Complete impact on the digital platforms and applications provided at the level of one or more governorates within a region, affecting one of the following beneficiaries Those affiliated to these governorates. Government Entities Businesses and Supply Chains Citizens and Residents	Financial losses of up to SAR 50,000 per hour, or 0.000575% of the total annual revenues generated by this service, whichever is greater.	Leads to a warning notice and a request for clarification of the incident from regulatory bodies, or a low-probability warning from authorities for potential legal violations.	Causes a negative impact on the entity's reputation, resulting in complaints from the beneficiary without media attention.	24 Hours
Low	Complete impact on the digital platforms and applications provided at the level of one or more center or body, such as: A university or institution in one of the Saudi governorates, of one of the following beneficiaries associated with these centers. Government Entities Businesses and Supply Chains Citizens and Residents	Financial losses of up to SAR 10,000 per hour, or 0000115% of the total annual revenues generated by this service, whichever is greater.	Results in a request for clarification from regulatory bodies without causing any legal violations.	Does not cause noticeable effects or attract media attention toward the entity.	48 Hours

Figure (59): BIA Matrix

In case of varying levels of impact between factors, the highest level will be considered.

**Targeted recovery times are subject to continuous review and updates.

Table (24) below provides an illustrative example on how to classify the government platforms and applications using the BIA Matrix:

#	Platform/ Application	Stakeholder Impact	Financial Impact	Legal and Regulatory Impact	Reputational Impact	Impact Level	Recovery Point Objective RTO
1	Unified National Platform	Critical	Low	Low	Moderate	Critical	8 Hours
2	Raqmi Platform	Critical	Low	Low	Critical	Critical	8 Hours

Table (24): Illustrative Example for Classifying Government Platforms and Applications.

Assessment of Risks and Threats

Risk assessment is a fundamental element in building a successful and effective Business Continuity Management System due to the key role this phase plays in identifying, analyzing and assessing risks or threats to the continuity of the government entity's operations. This phase also helps in identifying critical and non-critical risks or threats and in developing plans to address these risks, incorporating these plans into the business continuity strategy.

It is important to highlight the distinction between risk assessment in business continuity, as mentioned above, and enterprise risk management. The enterprise risk management process contributes to identifying a wide range of risks that may impact the operations of the government entity, assessing, analyzing and measuring their impact and likelihood, and developing appropriate treatment plans. In contrast, risk assessment within business continuity focuses on service/operation disruptions, which directly affect the ability of the government entity's employees to perform essential/critical tasks and activities.

Example: Disruption of communication between the main data center and one of the government entity's buildings could lead to the loss of access to the government entity's systems. For more details on the risk assessment phase, please refer to section (5.2.5.2).

The Business Continuity Management Unit is responsible for assessing and classifying risks within the government entity. Risks can be categorized based on the assessment results into several groups according to the type of resources supporting critical operations, as shown in (Figure 60):

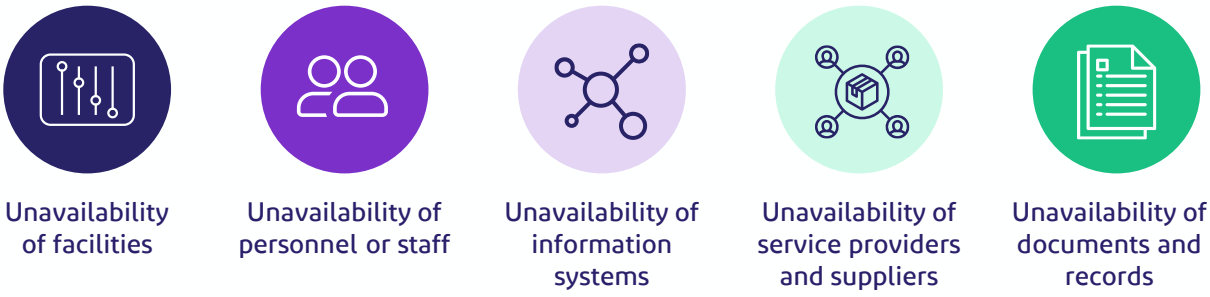


Figure 60 - Example of Risk Assessment Categories Based on Resources

Based on the risk and threat assessment and the deliverables of the Business Interruption Analysis (BIA), the business continuity strategy is developed, in alignment with the government entity's strategy. The strategy defines the solutions to be implemented to increase the efficiency of the government's business continuity or its ability to recover its operations according to the targeted recovery times. The strategy includes details about the resources needed to implement these solutions, which extend beyond financial resources to include human resources, equipment, systems, facilities, and other resources.

5.2.5.2.3 Building Business Continuity Plans

The BIA phase is the cornerstone of the business continuity system. During this phase, the procedures or operations within the government entity are analyzed, critical ones are identified, recovery priorities are set, and business continuity plans are developed accordingly. This phase includes the following plans:

- Business Continuity Plans for Different Units within the Government Entity

Business Continuity Plans primarily focus on restoring the operations of departments with critical procedures whose disruption could negatively affect the entity. At least one plan is created for each department with critical procedures, and a copy of the plan is available with all recovery teams within the department. The business continuity recovery plan includes all critical procedures and recovery times, alternative procedures and resources and their activation or provision mechanism, the internal and external communication system during disruptions, as well as all human and technological resources and equipment needed for service recovery. These plans clarify all internal and external dependencies of the procedures or services.

These plans focus directly on the technological and communication systems that support the continuity of critical procedures within the government entity. It is important to ensure that ICT disaster recovery plans are developed in alignment with the requirements for recovering critical procedures. The ICT disaster recovery plans also document all teams and roles responsible for activating or supporting the system recovery and rebooting. If there are gaps between the technological capabilities for service recovery and business requirements, these gaps should be included in the business continuity strategy, along with proposed solutions to reduce these gaps.

- Crisis Management Plan

This plan primarily focuses on crises that the government entity might face and how to address them in a comprehensive manner. The plan includes potential scenarios, such as, but not limited to, incidents that led to significant losses (financial, reputation, operational, security and safety, etc.), along with mechanisms to handle each incident. It also includes tasks and responsibilities of crisis management team members and relevant parties, indicators for activating recovery plans, and response teams. Further, the plan includes stakeholders and external entities that should be informed during a crisis.

- Media Communication and Response Plan

This plan focuses on internal and external communication plans, and identifying stakeholders involved in communication during a crisis or incident. It defines the messages to be communicated, the official spokesperson, communication channels, and how to handle risk scenarios that impact the government entity's reputation in the proper manner. The plan also includes monitoring developments on social media regarding the incident and how to address them, if necessary.

- Emergency Response Plan

The emergency response plan is an essential part of the business continuity system. It aims to ensure the government entity's ability to respond effectively to various types of emergencies (fires, floods, power outages, internet disruptions, etc.). Based on this plan, the government entity can ensure a reduction in the negative impact of the emergency on operations, protect its reputation, and improve its ability to adapt to crises.

The structuring of incident response plans is the process of determining goals, tasks, responsibilities and resources required to handle a potential or ongoing incident. Some of the key activities and procedures involved in structuring include:

- **Risk Analysis:** Assessment of assets, threats and the possible impact of incidents on the government entity.
- **Prioritization:** Identifying the activities, processes and services that should be protected and restored in the event of an incident.
- **Identification of Roles and Responsibilities:** Identifying the teams and individuals responsible for implementing the response plan, and determining the levels of authority, delegation and coordination between them, as well as the escalation mechanism.
- **Setting Procedures:** Identifying the steps and guidelines necessary to recognize, respond to, reduce, investigate and recover from an incident, and developing procedures for dealing with external parties.
- **Provision of Resources and Equipment:** Identifying and providing the resources and equipment needed to support the response plan.
- **Creating Contact Details:** Identifying the contact tree and contact information, and testing it periodically.
- **Testing and Reviewing the Plan**: Testing the effectiveness and efficiency of the response plan by conducting exercises, and reviewing and updating the plan regularly.

- Teams Participating in the Business Continuity Management System

In the business continuity system, there are several teams that play a crucial role in handling incidents. These teams work harmoniously and integratively to ensure business continuity, maintain security, safety, stability, and sustainability of the government entity's operations. However, the names and responsibilities of these teams may vary depending on the type and nature of the incident and the government entity. The most important teams include:

- Business Continuity Teams

The Business Continuity Team ensures the continuity of the entity's essential operations and services, and restores interrupted services within a specified time frame, not exceeding the targeted recovery time. The Incident Response Team serves as the link to crisis management and reports to the Crisis Management Team, when necessary.

- ICT Disaster Recovery Team

The ICT Disaster Recovery Team ensures the continuity of technological systems and digital services, working to restore conditions, and identify risks and mitigate their impact. This team follows guidelines, reports to the Crisis Management Team, and documents lessons learned to avoid future occurrences.

- Incident Management Team

The Incident Management Team responds immediately when an incident occurs to ensure the safety of the government entity's personnel, protect its assets, follow directives, report to the Crisis Management Team, and manage the incident across various involved teams.

- Crisis Management Team

The Crisis Management Team begins its work based on instructions from the leader or the responsible official (or their representative) within the government entity to assess the potential impact on the entity's critical resources and operations, making strategic and tactical decisions. Accordingly, a decision is made to activate the Business Continuity Plan and determine the expected recovery time.

- Emergency Response Team

The Emergency Response Team is responsible for the initial response to the emergency, with the aim of reducing its impact on people, and the entity's property and environment. This team consists of trained individuals equipped with the necessary tools and resources for rapid and effective intervention. It follows the entity's emergency plan, Emergency Response Team consists of the security and safety department and facilities department.

- Communication and Media Response Team

This team is responsible for preparing and executing the communication and media response plan for the incident, which includes: Identifying the targeted audience, key messages, appropriate channels and means of communication, and assessment and review of the effectiveness of communication and awareness event. Communication and Media Response Team handles internal and external communication, informs stakeholders during and after the incidents, follows directives, and reports to the Crisis Management Team.

- Logistical Support Team

This team provides resources, equipment, and services necessary for response and recovery teams, such as: Business Continuity Teams, Crisis Management Teams, and Emergency Response Teams.

- Assessment and Analysis Team

This team collects, analyzes and provides information related to the emergency, and its impact on people, property, environment and infrastructure. It provides recommendations and suggestions to other teams for making appropriate decisions. The Assessment and Analysis Team reports to relevant administrative units, such as: Facilities, Safety and Security Department, Technical Support, and Cybersecurity.

5.2.5.3 Verification Phase of the Business Continuity Management System

To ensure that the policies, plans and strategies of Business Continuity align with the government entity's goals and the priority of restoring its critical operations or procedures, the Business Continuity Management System must undergo a continuous verification process. This involves regular reviews, continuous testing, and different scenarios to identify gaps and shortcomings, while training and raising awareness among those responsible for the system. Figure (61) outlines the exercises and tests life cycle.

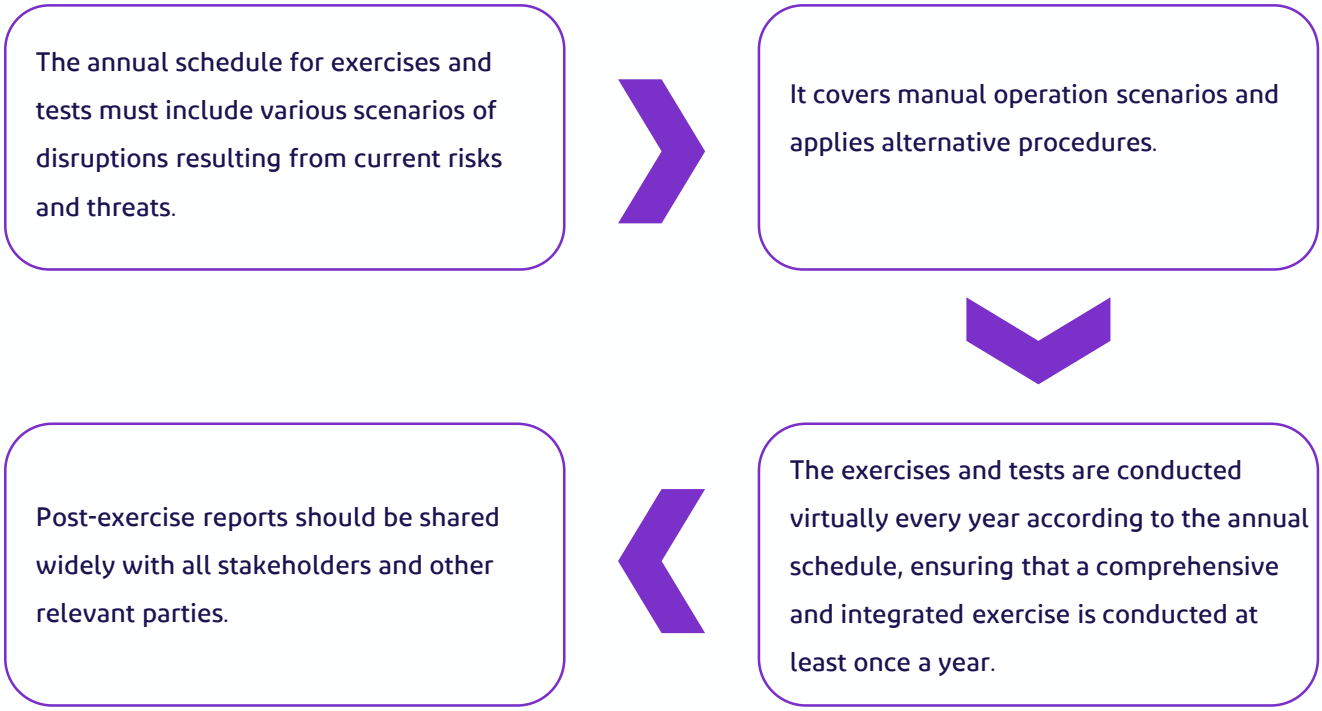


Figure (61): Example of Exercises and Tests Life Cycle

5.2.5.3.1 Exercises and Tests Related to the Business Continuity Management System

An annual specialized training plan is developed for all those involved in the Business Continuity Management System. A training plan for conducting tests regularly is also created for stakeholders and relevant parties to ensure that the exercises and tests are effectively applied to verify the efficiency of the business continuity plans and solutions. Exercises and tests are key to the success of business continuity plans in all their forms. Tests should not focus solely on specific plans but should cover all business continuity plans and recovery teams. It is recommended to conduct several tests annually, covering different scenarios based on the risk and threat register of the the government entity.

ICT Recovery Plans Readiness Tests

ICT business continuity plans are tested to ensure that they are prepared to deal with any type of possible disruption, on an ongoing and periodic basis to ensure business continuity and uninterrupted digital services. The most important types of ICT readiness tests include:

- Tabletop Exercises
- These exercises gather the relevant participants in the plan and focus on a specific incident. Each person assumes a role and plays out a series of incidents. The entity conducts various methods to pressure the participants, by introducing system failures and work stoppages, which may occur during real incidents, in order to observe their reactions.

- Specific Procedural Tests
- Procedure testing aims to test the presence of one or more specific procedures within the government's ICT readiness plan, as intended, or assess the need for development.

This type of testing could involve assessing the functionality of communication systems within the government entity.

- Full-Scope Exercises
- These exercises assess the full operational effort of the government's digital and communication systems concerning a specific incident. The exercise may include elements of preparedness efforts, such as: Coordination with other entities.

- Crisis Management Plan Testing
- The objective of testing crisis management plans is to assess their effectiveness and ensure that they are ready to handle a variety of emergencies or disasters. This test typically involves organizational and operational processes to ensure an effective response in the event of an unforeseen incident.

- Emergency Plan Testing
- Testing emergency plans involves evaluating their readiness and competence in dealing with emergencies. This test includes identifying the strengths and weaknesses of the plans and ensuring that the relevant teams are capable of managing emergencies effectively.

5.2.5.4 Business Continuity System Corrective Phase

In this phase, efforts are made to correct the gaps and deficiencies identified during the verification phase to ensure the effectiveness of the business continuity system and align it with the operational and strategic objectives of the government entity.

5.2.5.4.1 Documentation and Continuous Improvement

Review of the Business Continuity Management System

It is essential to periodically assess the relevance, efficiency and effectiveness of the Business Continuity Management System, or whenever there is a significant change in the government entity. This review is carried out through the development of performance indicators, continuous evaluation of reports from business continuity plan exercises and tests, and the ongoing process of development, improvement and correction. Review activities include:

- Setting appropriate performance indicators for the system and regulatory requirements.
- Monitoring the achievement of policies and objectives of the Business Continuity Management System.
- Evaluating the performance of processes, procedures and functions that protect the critical operations of the Business Continuity Management System.
- Proactively measuring performance to monitor compliance with laws and regulatory requirements, as well as assessing past performance during failures, incidents and violations.
- Recording data and monitoring results to facilitate subsequent analysis for corrective actions.

Business Continuity Performance Indicators

Business continuity performance indicators are essential for the success of the Business Continuity Management System and achieving its goals. These indicators must be directly aligned with the principles and strategy of the government entity to enable sustainability and proper execution thereof. Figure (62) below outlines the alignment process and methodology.

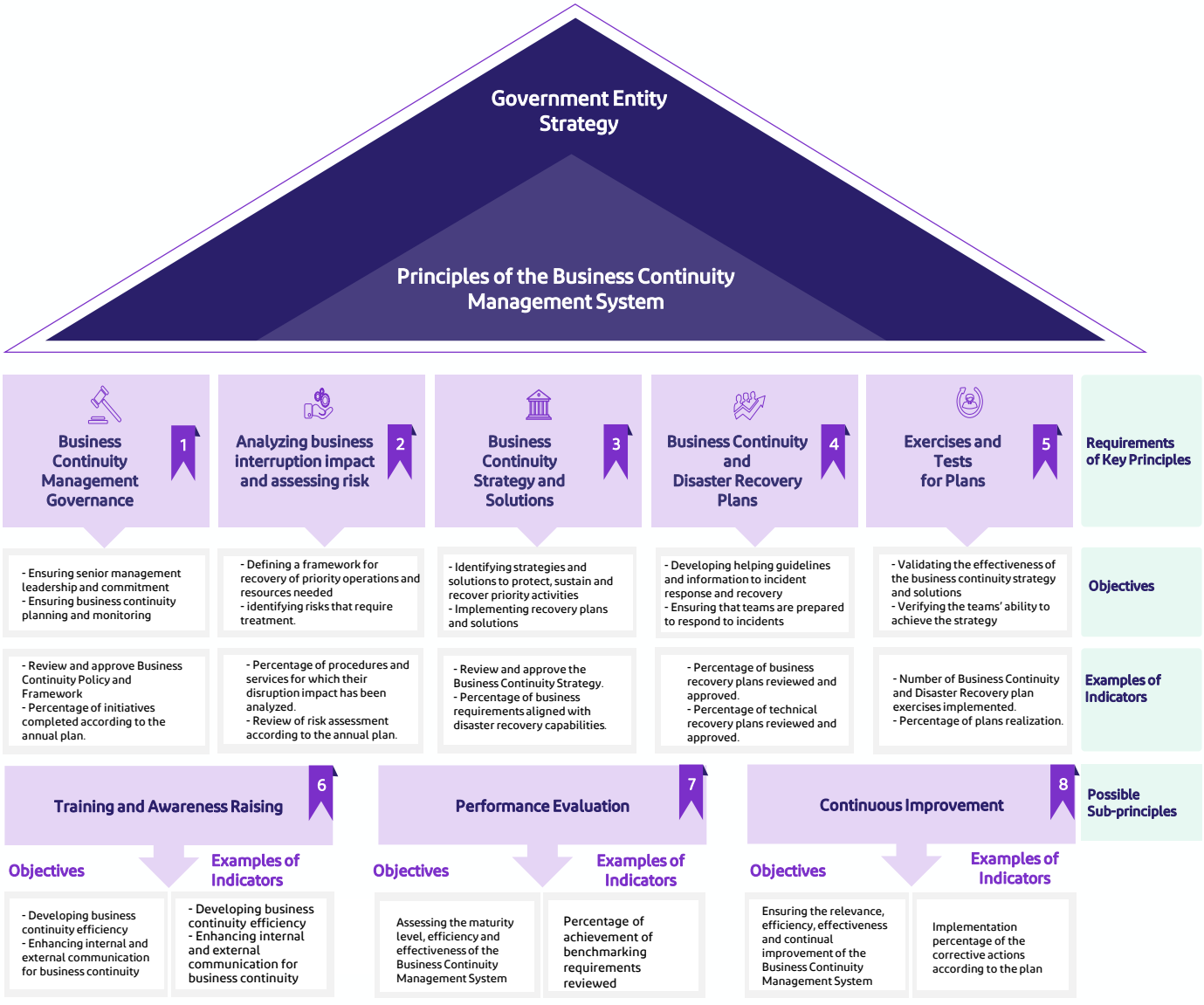


Figure (62): Illustrative Example of the Alignment Process and Methodology

- Compliance and Corrective Actions

Corrective actions are built upon the identified gaps and deficiencies in the Business Continuity Management System, focusing on addressing these gaps through the implementation of corrective and improvement measures to enhance the system's efficiency within the government entity. In adherence to best practices, the Business Continuity System undergoes an annual review by either an internal or external auditor with the necessary qualifications and expertise.

- Review and Audit

Regular internal and external reviews and audits of the Business Continuity Management System and recovery plans (as per the audit plan) are essential for continuous improvement. The outcomes of audits yield clear reports and corrective suggestions aimed at refining operations and plans. Audits verify the presence, coverage, relevance, application, testing, updating, and documentation of the plans. The audit results provide an accurate overview of the current level of business continuity planning within the government entity. To ensure impartiality, individuals responsible for internal audits should not be involved in the Business Continuity Management System's direct operations. Internal audits typically involve reviewing various functions or processes annually, incorporating continuity and recovery plan assessments into the annual audit plan. Alternatively, the review can be conducted by an independent and reliable external party.

In a comprehensive review of the Business Continuity Management System, the results of the internal and external audits are escalated to senior management and the steering/supervisory committee for review. This step aims to ensure that corrective actions are taken and to continuously improve the relevance, efficiency and effectiveness of the Business Continuity Management System to ensure that the desired results are achieved. Continuous improvement is planned to integrate the Business Continuity Management System into the core activities, operations and services of the government entity.

- Administrative Review

The administrative review of the business continuity management system is carried out continuously within the government entity to ensure alignment with the directions of the senior management and the strategic objectives of the entity.

The responsible administrative unit ensures the availability of the resources required for the development of the business continuity management system. This is why it is important to obtain updated information about changes in the operating environment, business requirements, risks within the government entity, the operational requirements of the Business Continuity Management System, and the current situation. Administrative review must be linked to process monitoring. The goal is to ensure that the operations of the Business Continuity Management System are appropriate, effective, and that their procedures are correct. The following topics, at a minimum, must be reported to senior management and the steering/supervisory committee regarding Business Continuity Management:

- Summary of realized disruptions requiring measures for the sustainability of the business continuity management system.
- Changes in the operating environment of the business continuity management system.
- Requirements for developing Business Continuity Management System metrics.
- Results of periodic reviews, and actions and support required.

06. Documentation Management

Structured preservation and archiving of documents and data using various technologies, including, but not limited to, as follows: Automation platforms for Risk Management and Business Continuity Management systems. Multiple storage media, such as shared folders and cloud storage services. Standardized templates within the systems. These technologies are key to maintaining accuracy, consistency, and efficiency, as well as ensuring the effectiveness and continuity of the Risk Management and Business Continuity Management systems in the government entity.

1. Documents and Data Archiving Mechanism

Developing a mechanism that outlines the method for preserving and archiving data, the tools and technologies used in Risk Management and Business Continuity Management, and the roles and responsibilities of relevant stakeholders. The mechanism also aligns these methods with internal policies related to data protection and classification within the government entity.

Illustrative Example: Archiving the system's documents and data in the shared folder on the cloud computing platform of the government entity, managing and granting access to the folder by the managers responsible for the systems, ensuring that a backup policy is in place.

2. Models of Risk Management and Business Continuity Management Systems

Standardized templates for the processes of Risk Management and Business Continuity Management Systems are created and used by the administrative unit's team in the government entity. These templates include, but not limited to, as follows: Risk registers, risk escalation and appetite forms, risk reports, risk dashboards, business impact analysis templates, business continuity testing reports, and others. This ensures the sustainability of risk management processes and facilitates continuous comparison and analysis of information.

3. Automation of Risk Management and Business Continuity Management Systems

Automation tools can be defined as systems or applications that include a set of workflows, data flows, and reports related to the procedures and activities of Risk Management and Business Continuity Management systems at the executive and operational levels of the entity. These tools facilitate the execution of tasks and activities related to risk management and business continuity, ensure transparency in governance processes, and provide stakeholders with effective and timely reports. This, in turn, guarantees strategic visibility for decision-makers to take the necessary actions promptly and in a manner that serves the government entity effectively.

07. Table of Definitions

The following terms and phrases shall have the meanings assigned thereto wherever stated herein; unless the context requires otherwise:

Term	Definition
DGA	Digital Government Authority (DGA).
Digital Government	Promotes administrative, organizational, and operational processes between the various government agencies in their transition to a comprehensive digital transformation to allow easy and effective access to government digital information and services.
Government Entities	Ministries, authorities, public institutions, councils, and national centers, including any additional form of public Agency.
Administrative Unit	A business unit within the organizational structure of the Agency, specializing in specific roles and responsibilities.
Controls	The controls specify the conditions that government agencies must comply with and what they must do to achieve the objectives and general provisions stated in the policy associated with them.
Digital Transformation	Digitally and strategically transforming and developing business standards and models that would rely on data, technologies, and ICT.
Risk Management System	The principles, frameworks, and processes followed by the organization in managing risks for digital government to achieve the strategic objectives of the organization.
Risk	The probability of an event occurring that will have negative or positive effects.
Incident	An incident that has consequences and implications that may affect the achievement of the entity's objectives either negatively or positively.
Internal and External Risks	Internal or external incidents that may affect the achievement of the entity's strategic objectives.
Risk Management	Applying strategies, policies, and procedures to prevent the emergence of new risks, reduce existing risks, and manage residual risks. By anticipating and identifying, analyzing, evaluating, prioritizing, monitoring and reviewing of the risks, and preventing and mitigating the negative effects resulting from them.
Risk Management Policy	The main document defines the governance and scope of risk management, along with risk management objectives and the roles and responsibilities of relevant parties.
Authority Matrix	A documented structure detailing the allocation of roles and responsibilities assigned for performing tasks.
Risk Management Strategy	The entity's approach to managing risks and identifying optimal solutions to minimize their impact on the entity.
Risk Appetite Level	The level, type, and magnitude of risks the entity can accept while ensuring the achievement of its objectives.

Risk Tolerance Level	Risk tolerance limits in proportion to the agency's risk appetite, after implementing risk mitigation measures.
Risk Management Framework	Methodology and mechanisms for identifying, analyzing, and evaluating risks, treating them, and following them up periodically at the entity.
Risk Assessment	A quantitative or qualitative approach to identifying, analyzing, and estimating the likelihood of occurrence and impacts of potentially risks, taking into account exposure factors, vulnerabilities, and vulnerability.
Control Measure	A policy, procedure, practice, process, or technology designed to reduce the likelihood and/or impact of risks.
Risk Owner	The party responsible for managing a specific risk within its jurisdiction and mandate, including anticipating, identifying, analyzing, assessing, prioritizing, monitoring, reviewing, preventing, mitigating, preparing for, responding to, and recovering from it in coordination with supporting and assisting entities.
Owner of Risk Response Plans	The individual or entity authorized to implement, execute and report risk treatment plans to the Risk Management Team and stakeholders.
Risk Champions	The resulting consequences in case a risk occurs within the various main departments of the entity, to coordinate, monitor, and execute risk management tasks and submit related reports.
Impact	The consequences and outcomes resulting from a risk when it occurs.
Likelihood	The extent to which a risk can occur and recur within a specific period of time.
Inherent Risks	Preliminary risks before implementing any mitigation measures to reduce the impacts resulting from them.
Residual Risks	Continuing risks after implementing prevention and mitigation controls, which require continuous work treat them.
Risk Matrix	A mechanism used during risk assessment to determine the level of risk based on the likelihood and possibility of the risk occurring versus the implications of the risk occurring.
Key Risk Indicators (KRIs)	A measure used to monitor changes in the level of risk exposure, and is used as an early warning sign for risks.
Risk Register	A document containing a list of risks, including all related data and information, such as: Risk Registration Date, Risk Code, Sector, Risk Owner, Risk Classification, Risk Description, Risk Occurrence Scenario, Likelihood Level, Impact Level, Risk Level, Key Risk Indicators, and Treatment Strategy and Plans.
Risk Trend	The direction in which inherent or residual risks move. For example, the severity of an inherent risk may increase, but after treatment, the severity of a residual risk may decrease. (Downward)
Compliance and Conformity	The entity meets the necessary requirements in the required manner.
Continuous Improvement	A recurring activity to enhance the performance of risk management and business continuity processes.
Senior Management	All individuals responsible for making strategic and fundamental decisions within the entity.
Contact Person	An entity, person or department that can be contacted to obtain information, support, or advice regarding a specific matter.

Contact Person	An entity, person or department that can be contacted to obtain information, support, or advice regarding a specific matter.
Quality Assurance	The process of evaluating the extent to which the outputs of the risk management system meet the entity's requirements and expectations.
Supply Chain Resilience Management	The application of strategies, policies and procedures necessary to strengthen the resilience of supply chains for essential services, goods and products provided by the entity. This ensures the availability of an acceptable level of services and products during disruptions or outages. It includes analyzing and mapping supply chains, identifying links and connections, assessing risks of disruption, defining resilience strategies, and responding to and recovery of emergencies.
Training	Building skills and competencies to increase employee performance in relation to specific roles or responsibilities .
Stakeholders	Parties and entities that influence and are influenced by the decisions, directions, procedures, objectives, policies and initiatives of the digital government and share some of its interests and outputs and are affected by any change thereon.
The Road Map	A detailed plan to guide and clarify progress in achieving initiatives and objectives.
Internal Auditing	A review of compliance with risk management controls, business continuity requirements, or policy mandates.
Resources	Resources include financial resources, information, skills, individuals, technologies, and solutions that the entity acquires and uses to achieve its organizational goals and objectives.
Self-Assessment	Internal review of the implementation of the risk management and business continuity system in order to develop an improvement action plan.
Awareness	Developing an understanding of the main risks and threats that can negatively affect the achievement of the entity's objectives.
Communication and Consultations	A set of ongoing and recurring processes within the entity aimed at obtaining or sharing information with stakeholders regarding risk management and business continuity.
Threats	Any possible cause of an act, conduct or event that could cause harm.
Beneficiary	Citizen, resident, visitor, government agencies, private sector organizations, or non-profit organizations inside and outside the Kingdom of Saudi Arabia that need to interact with any agency to obtain any of its services.
Risk Treatment	Strategies for treating risks, which include: Risk acceptance, avoidance, transfer or treatment/mitigation.
Risk Acceptance	Accepting the consequences and implications of risks within appetite risk levels.
Risk Avoidance	Preventing risk by not initiating or halting activities that could lead to harm or loss.
Risk Mitigation	Reducing the likelihood or impact of risk until it reaches acceptable levels.
Risks Transfer	Transferring the liability or burden of loss to another party through legislation, contract, insurance or other means

Supply Chains	Networks connecting exporters, suppliers, related entities, distributors, beneficiaries, resources, processes, and technologies. These networks facilitate the acquisition of inputs and materials necessary for production, manufacturing, processing, and distribution to deliver a service or product to beneficiaries.
Procedures	Specific, standardized and detailed steps through which tasks, processes, or activities related to risks and business continuity are executed, based on relevant policies and standards.
Business	The necessary tasks and efforts carried out by the entity to achieve the objectives related to risks and business continuity.
Processes	Interconnected, overlapping, and interactive activities aimed at achieving specific outcomes in risk management and business continuity, based on the approved policies and procedures.
Competence	The ability to utilize physical resources, knowledge, expertise, and skills required for planning, organizing, managing, monitoring, and overseeing risk management and business continuity.
Effectiveness	The capability to achieve the primary objectives of risk management and business continuity through effective planning, cost control, execution, and results measurement based on the approved indicators.
Workshop	A discussion-based exercise that guides participants or provides an overview of plans, policies, legislation, resources, capabilities and capacities.
Training	An operational exercise used to test or practice a specific procedure, role, or mechanism within a designated work team.
Business Continuity	The resources, capabilities, procedures, and actions necessary to continue providing core services and products at pre-determined levels and within an acceptable time frame in the event of disruption
Business Continuity Strategy	The Agency's approach is to choose appropriate solutions to continue providing core services and products during a disruption, as well as its recovery strategy after the situation.
Business Continuity Management System	An integrated administrative system that aims to: establish, implement, operate, maintain, monitor, review, and develop the necessary measures for an agency to continuity providing its core services and products.
Business Continuity Plan	A document that specifies the general framework for managing, coordinating, and directing resources, procedures, and human and technical capabilities to respond to disruptions, continue providing core products and services and recover as quickly as possible for the continuity of the Agency's business.
Organizational Resilience	The entity's ability to absorb and adapt in a changing environment to enable it to achieve its objectives, survive, and thrive.

ICT Disaster Recovery (DR)	The ability of the entity's ICT disaster recovery elements – including all digital technologies – to restore its critical systems to an acceptable level within a predetermined time frame following a disruption.
Recovery Time Objective (RTO)	The time period the entity takes to restore its product, service, activity, or resources after an incident.
Recovery Point Objective (RPO)	The point to which information used in an activity is restored to enable the resumption of operations.
Maximum Tolerable Period of Disruption (MTPD)	The amount of time after which the negative consequences resulting from the failure to deliver a product, service, or activity become unacceptable.
Minimum Business Continuity Objective (MBCO)	The minimum level of product or service considered sufficient to enable the entity to achieve its organizational objectives after a disruption.
Business Impact Analysis (BIA)	Analysis of business processes and activities related to providing core services products, and the effects of disruption of those processes.
Crisis	An abnormal and unstable situation that threatens the strategic objectives, reputation or survival of the entity.
Compliance	The extent to which the entity meets the mandatory requirements.
Disruption	An incident, whether anticipated or unanticipated, causes an unplanned, negative deviation from the expected delivery of products and services according to an Agency's objectives.
Administrative Review	An evaluation or reconsideration by management of a specific situation or topic.
Media Response Plan	A plan that provides the entity with details about its media response following an incident, including the communication strategy.
Remote Work	A work system where an employee performs his job duties for the interest of his employer and under its supervision, at a location other than the usual workplace within Saudi Arabia, whether full-time or part-time, using ICT technologies.
Performance Assessment	An approach used to verify the efficiency of employees in performing tasks, roles, and responsibilities to achieve the defined objectives.
Priority Activities	Classifying an activity as urgent to avoid unacceptable impacts on operations during a disruption.
Process	A set of interrelated or interacting activities that turn inputs into outputs.

Recovery	Documented procedures to restore business activities from temporary measures adopted during and after a disruption.
Testing	An activity or procedure aimed at measuring the capabilities and effectiveness of a specific strategy or plan, based on predefined criteria. (It should include success or failure elements).
Enterprise Risk Management	Enterprise Risk Management involves understanding, analyzing and addressing risks to ensure that entities achieve their objectives.
Business Continuity Champions	Representatives of business continuity management in various key departments within the entity, to coordinate, monitor, and implement business continuity management activities and report related matters.
Security Incidents	Any digital or physical breach that threatens the confidentiality, integrity or availability of the entity's sensitive information or data systems.

08. Table of Abbreviations

The following terms and phrases shall have the meanings assigned thereto wherever stated herein; unless the context requires otherwise:

Term	Definition
RTO	Recovery Time Objective
RPO	Recover Point Objective
MTPD	Maximum Tolerable Period of Disruption
MBCO	Minimum Business Continuity Objective
BIA	Business Impact Analysis
MCA	Multi-Criteria-Analysis.
ICT	Information and communication technology
HSSE	Health, Safety, Security and Environment

09. References and Sources

The section shows the most prominent references and regulations that were referred to during the preparation of this Guideline:

#	Reference
1	Controls of Risk and Business Continuity Management For Digital Government https://dga.gov.sa/ar/Controls_Of_Risk_and_Business_Continuity_Management_For_Digital_Government
2	ISO 31000:2018 https://www.iso.org/
3	ISO 31010:2019 https://www.iso.org/
4	ISO 27001:2022 https://www.iso.org/
5	Frameworks and Guidelines issued by the National Risk Council.
6	Risk Management in Organizations under the Supervision of COSO Committee https://www.coso.org/
7	Institute of Risk Management, https://www.theirm.org
8	Institute of Internal Auditors https://www.theiia.org
9	The United Nations https://www.un.org
10	Risk Management Manual issued by the Saudi Ministry of Finance
11	National Cybersecurity Authority https://nca.gov.sa
12	Information Technology Infrastructure Library (ITIL)
13	Australian/New Zealand Standard (AS/NZS 4360:2004) https://www.standards.org.au/standards-catalogue/standard-details?designation=as-nzs-4360-2004
14	UK Government Risk Management Guide – The Orange Book https://www.gov.uk/government/publications/orange-book
15	Guidance Note for Risk Appetite and Tolerance Levels – The Orange Book https://www.gov.uk/government/publications/orange-book

15	Guidance Note for Risk Appetite and Tolerance Levels – The Orange Book https://www.gov.uk/government/publications/orange-book
16	Risk Reports Practices Guideline https://www.gov.uk/government/publications/orange-book
17	NASA Independent Verification and Certification Program Risk Management Manual https://www.nasa.gov/ivv-ims-supporting-documents/
18	British Columbia-Canada Public Sector Risk Management Manual https://www2.gov.bc.ca/gov/content/governments/services-for-government/internal-corporate-services/risk-management
19	Information Systems Control and Audit Association – ISACA https://isaca.org/
20	Organization for Economic Co-operation and Development (OECD) https://www.oecd.org/
21	The Resilience Index to measure the level of readiness in risk and emergency management and business continuity issued by the General Secretariat of the National Risk Council.
22	ISO 22301:2019 https://www.iso.org/
23	ISO 22330:2018 https://www.iso.org/
24	ISO 22317:2015 https://www.iso.org/
25	ISO 22398:2013 https://www.iso.org/

10. List of Figures and Tables

10.1 List of Figures

10.2 List of Tables

11. Annexes

11.1 Indicative List of Potential Risks to Government Entities

The following list provides examples of risks and their main categories that the government entities may face:

1. Strategic Risks

#	Sub-Risk Category	Risk
1	Strategy and Planning Risks	Lack of reliance on accurate data during the strategic planning process due to lack of data collection and analysis systems. This leads to ineffective strategic decisions.
		Delay in the completion of major projects due to poor planning or lack of resources, which may lead to delay in achieving the strategic objectives, and affect the government entity's reputation.
2	Governance Risks	Weak coordination and integration between the various administrative units due to the lack of clear communication mechanisms. This may lead to the disruption of initiatives and projects' execution, as well as delays in achieving objectives.
3	Projects and Programs Risks	Delays in approving initiatives due to weak project allocation and budget distribution for initiatives and operational projects. This may affect business operations and increase the likelihood of not achieving the strategic objectives of the government entity.
4	Reputation Risks	The spread of negative comments on social media due to poor responsiveness to beneficiary complaints. This may lead to damage to the reputation of the government entity.
5	Performance Indicators Risks	Using inaccurate performance indicators due to weak data accuracy. This may result in the inability to make correct strategic decisions.
6	Business Development Risks	Failure to link performance indicators with the strategic objectives of the entity due to weak alignment between strategic planning and performance evaluation. This may lead to ineffective improvement measures and failure to achieve goals.

Table (25): Examples of Strategic Risks

2. Legal and Compliance Risks

#	Sub-Risk Category	Risk
1	Legal Risks	Exposure to legal cases due to violations in operations or poor contract management. This may result in fines and negatively impact the reputation of the government entity.
2	Policy and Procedure Risks	Ineffective policies and procedures due to the failure to adopt best practices and standards. This may lead to inconsistencies in implementing procedures and regulations.
3	Non-Compliance with National Laws and Regulations Risks	Weak compliance with internal policies and procedures due to lack of awareness and oversight. This could negatively impact the overall performance of the government entity.
4	Roles and Responsibilities Risks	Overlap of roles and responsibilities in business operations due to poor task allocation. This may result in conflicts of interest and difficulty in accountability.
5	Fraud Risks	The possibility of fraud in financial transactions due to weak internal controls and security systems. This may lead to financial losses for the government entity.
6	Professional Conduct Risks	Non-compliance with ethical professional standards due to lack of awareness and insufficient training. This may lead to legal violations and negatively affect public trust in the government entity.
7	Transparency and Control Risks	Weak effectiveness of internal control systems due to insufficient resources. This could lead to legal and financial risks and negatively impact the overall efficiency of the government entity.

Table (26): Examples of Legal and Compliance Risks

3. Operating Risks

#	Sub-Risk Category	Risk
1	Internal Technology Risks	Disruption of technological systems or infrastructure due to inefficient maintenance and updates, or non-renewal of licenses. This may lead to delay or disruption of business performance in the government entity.
2	Human Resources Risks	Lack of necessary human resources and competencies for operations due to challenges in recruitment or training. This may reduce operational efficiency and quality of services provided by the government entity.
3	Financial Risks	Weakness in supply chain management and procurement due to poor planning and coordination. This may lead to increased costs and financial losses to the government entity.
4	Human Resources Risks	High employee turnover rates due to job dissatisfaction. This may increase workload and disrupt business operations in the government entity.
5	Supply Chain Risks	Lack of diversity in supply sources due to over-reliance on a limited number of suppliers. This may negatively impact operations in the event of supplier disruptions.
6	Assets Management Risks	Loss or theft of government entity assets due to insufficient security measures. This may lead to financial loss and impact the services provided by the government entity.
7	HSSE Risks	Accidents or injuries in the workplace due to inadequate safety measures or training. This may result in business disruptions, human loss, and damage to the government entity's reputation.
8	Business Continuity Risks	Inability to respond effectively to emergencies or crises due to the absence of defined emergency plans and practices. This may cause delays or disruptions in the government entity's operations.

Table (27): Examples of Operational Risks

4. Digital Risks

#	Sub-Risk Category	Risk
1	Cloud Computing Risks	Non-compliance with data and privacy regulations due to storing data in different geographical locations. This may lead to legal consequences and financial penalties on the government entity.
2	Assets Risks	Weak asset management efficiency due to the absence of effective asset management strategies. This may lead to financial losses for the government entity.
3	Digital Fraud Risks	The possibility of beneficiaries of government digital services being exposed to fraud due to lack of awareness and weak security settings in systems, services, and platforms. This may harm the government entity's reputation and lead to loss of trust among beneficiaries.
4	Digital Transformation Risks	Delay in adopting modern technologies due to lack of innovation and technological development strategies. This may reduce operational efficiency and harm the government entity's reputation.

Table (28): Examples of Digital Risks

5. Cybersecurity Risk

#	Sub-Risk Category	Risk
1	Data Confidentiality Risks	Exposure of technical systems to cyberattacks due to weak cybersecurity protection and inadequate security measures. This may lead to data leaks and harm the government entity's reputation.
2		Possible unauthorized access to systems due to weak efficiency in access control settings for remote work systems. This may compromise data confidentiality.
3		Non-compliance with data protection standards due to lack of awareness and necessary procedures. This may lead to data breaches and potential legal penalties on the government entity.
4	Data Integrity Risks	Lack of security awareness among employees due to the absence of awareness programs and workshops. This may facilitate security breaches in the government entity.
5		Lack of regular security updates for systems and applications due to non-enforcement of policies and procedures. This may lead to system failures and vulnerability to breaches.
6		Difficulty in detecting or tracking cyberattacks due to lack of monitoring activities and systems. This may lead to disruption of sensitive systems and harm the entity's reputation.
7	Data Availability Risks	Lack of data backup systems due to non-compliance with backup policies. This may result in data loss and disruption of operations of the government entity.

Table (29): Examples of Cybersecurity Risks

11.2 Professional Certifications for Risk Management and Business Continuity Systems

Table (30) below outlines certifications related to risk management and business continuity systems, Issuing Body, and the suggested experience level required for certification:

#	Certificate	Issuing Body	Level of Experience
1	Professional Risk Manager (PRM)	International Association of Risk Managers - PRMIA	Beginner
2	Certified Risk Specialist (CRS)	International Academy of Business and Financial Management - IABFM	Beginner
3	ISO 31000, Introduction	International Organization for Standardization - ISO	Beginner
4	ISO 31000, Foundation	International Organization for Standardization - ISO	Beginner
5	Financial Risk Manager (FRM)	Global Association of Risk Professionals - GARP	Advanced
6	Risk Management Professional (PMI-RMP)	Project Management Institute - PMI	Advanced
7	Operational Risk Manager (ORM)	International Association of Risk Managers - PRMIA	Advanced
8	Certified Risk Management Professional (CRMP)	Institute for Risk and Resilience - RISKS	Advanced
9	Certified Risk Manager (CRM)	National Alliance for Education and Research - SCIC	Advanced
10	ISO 31000, Risk Manager	International Organization for Standardization - ISO	Advanced

11	Enterprise Risk Management Certified Professional (ERMCP)	Enterprise Risk Management Academy - ERMA	Expert
12	ISO 31000, Lead Risk Manager	International Organization for Standardization - ISO	Expert
13	International Certificate in Enterprise Risk Management (IRMCert)	Institute of Risk Management - IRM	Expert
14	Certification in Risk Management Assurance (CRMA)	Institute of Internal Auditors - IIA	Expert
15	Certification in Risk and Information Systems Control (CRISC®)	Information Systems Control and Audit Association- ISACA	Expert
16	Certified Business Continuity Professional (CBCP)	DRI International	Beginner
17	ISO 22301 Business Continuity Management	International Organization for Standardization - ISO	Beginner
18	Emergency Management and Continuity Professional (EMCP)	American Society of Safety Engineers - ASSE	Beginner
19	Business Continuity and Resilience Award (CBRA)	Business Continuity Institute - BCI	Advanced
20	Business Continuity Management Specialist (BCMS)	International Consortium for Organizational Resilience - ICOR	Advanced
21	Certified Emergency Manager (CEM)	International Association of Emergency Managers - IAEM	Advanced
22	Master Business Continuity Professional (MBCP)	Disaster Recovery Institute International - DRII	Expert
23	Certified Business Continuity Manager (CBCM)	Business Continuity Institute - BCM	Expert
24	Certified Emergency Management Professional (CEMP)	International Association of Emergency Managers - IAEM	Expert

Table (30): Risk Management and Business Continuity System Professional Certifications

11.3 Common Mistakes in Developing Business Continuity Plans

- Failure to define the relationship between the maximum data loss tolerance for ICT system and the targeted recovery time during emergencies. Accordingly, there is no clear data of the time that the government entity will take to restore critical tasks after a major disruption of digital services and ICT systems.
- The government entity has not made a decision on which ICT systems are given higher priority than other systems in the government entity. There may be limited capacity for the supplier to retrieve systems more quickly, and in real time. Therefore, the priorities of the systems in the government entity must be determined.
- Failure to develop systematic maps of interconnections and dependencies between ICT systems, and therefore data exchange is not fully mapped between ICT systems or systems that must be operational before other systems can operate.
- Failure to clarify the department or unit responsible for coordinating the response to ICT emergencies.
- Failure to test the government entity's emergency plans, which makes it unprepared to implement the government entity's internal ICT emergency plans in the event of an emergency.
- Lack of plans to restart the ICT system, due to the lack of an adequate description of the necessary activities. Therefore, it affects recovery in cases of disruption and emergency.

11.4 Example of ICT Disaster Recovery Methodology

Phase	Description
1. Security Incident Preparation	A plan must be developed to prevent and respond to security incidents.
2. Detection and Analysis	Determining whether a security incident has occurred, and defining its severity and type.
3. Containment and Eradication	Stopping the incident's impact before further damage occurs.
4. Post-Incident Recovery	A debrief with all involved parties is mandatory after a major incident and recommended after less severe incidents to manage incidents in a more effective and efficient way.

11.5 Example of Incident Response Structure

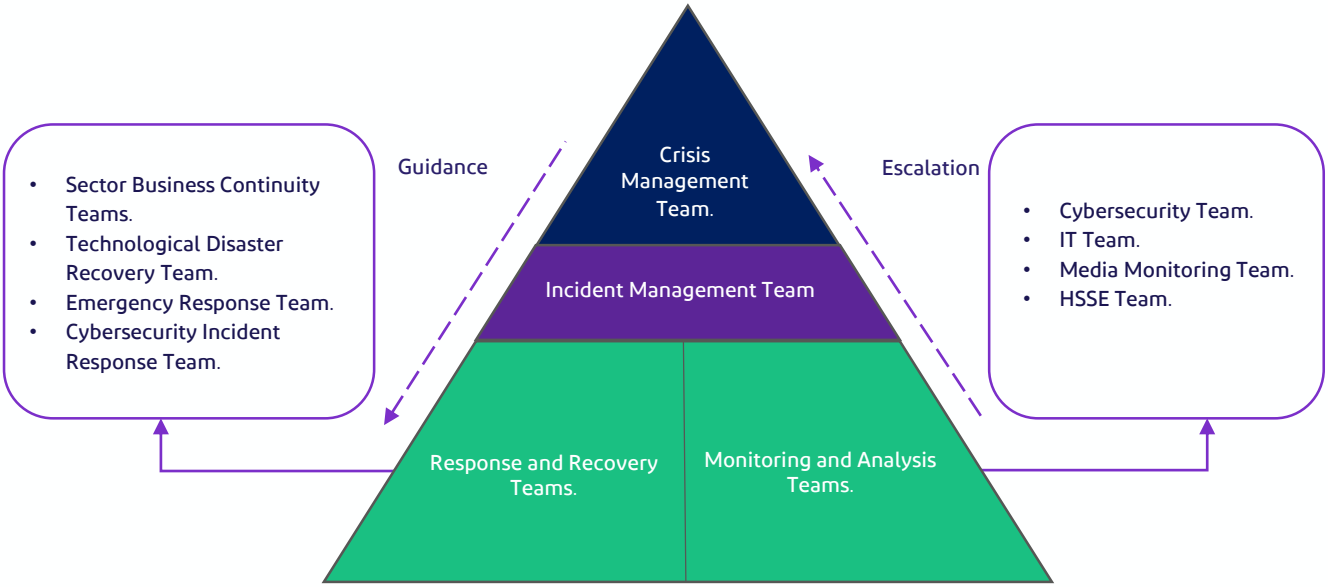


Figure (63) - Drawing 1: The organizational structure of the management, response and recovery teams for different incidents

Figure (64) - Drawing 2: The structure and interrelationship of the plans followed for the different levels incidents

هيئة الحكومة الرقمية
Digital Government Authority

DGA.GOV.SA