Digital هيئة
Government الحكومة
Authority الرقمية

The Guideline

for Business Continuity Management in Digital Government

March 9 ,2023

Document Type: Guideline

Document Classification: public

Issue No: 2.0

Document No: DGA-1-2-5-209

Table of Contents

Table of Contents

1. Introduction

In order to achieve the objectives of Vision 2030 to enhance the reliability and continuity of digital services in government entities, the Digital Government Authority has prepared the " Guidelines of Business Continuity Management in Digital Government" to emphasize the importance of adopting the principles of Business Continuity given the rapid changes and current events surrounding digital business and services in government entities, which could impact its business continuity and the beneficiaries' experience.

Enabling Business Continuity Management is a basic principle in ensuring the sustainability of the government entity's business and its ability to recover business and services through specific resources and technologies within a specific time. Business Continuity Management and Disaster Recovery contributes to maintain the ability of the government entity to deal with unexpected risks and reduce the possibility of their occurrence or impact, through the fast response, and improve stakeholders' trust and empower the government entity to effectively activate Media Communication Plans during crises. The system also helps to raise the entity's maturity level until it reaches the stage of organizational resilience to face crises and disasters, and reduces the financial, legal, regulatory, operational and reputational consequences of the government entity.

This document is a reference for government entities to help comply with "Controls of Business Continuity Management for Digital Government" issued by the Digital Government Authority "DGA" in order to raise the level of effectiveness of implementing and operating services digital in government entities.

This guideline has been prepared for the purpose of guidance and to provide general guidance and does not represent professional advice and does not replace the requirements in local and international standards.

Business continuity management operations in the government entity is based on the facts and circumstances surrounding its operating environment, relevant external parties, regulatory requirements for Business Continuity Management Standards issued by the authority and other regulatory entities, and international best practices.

2. Guideline Objectives

This guideline will contribute to enabling entities to :

1. Have knowledge and understanding of the applying the business continuity management standards for digital government in government entities.
2. Help to reduce the likelihood or impact of interruptions to the services.
3. Raise readiness by preparing, responding to and recovering from interruptions.
4. Continuity of critical services and procedures during accidents and crises.
5. Comply with regulatory requirements.
6. Raise the level of integration between government entities and enhance resilience and resilience at the national level.

3. Guideline Scope

Enhance the resilience of government entities to respond to any disruptions and enable them to recover their main operations and services through guiding government entities, suppliers and operators of digital government services to implement and maintain an effective management system that provides the necessary capabilities to continue the business operations while facing any disruption, as well as comply with legal and regulatory requirements.

Additionally, this guideline provides guidance to enhance business continuity practices in government entities as per the methodology of **Plan, Do, Check, Act** (PDCA), as shown in the Figure (1) below:

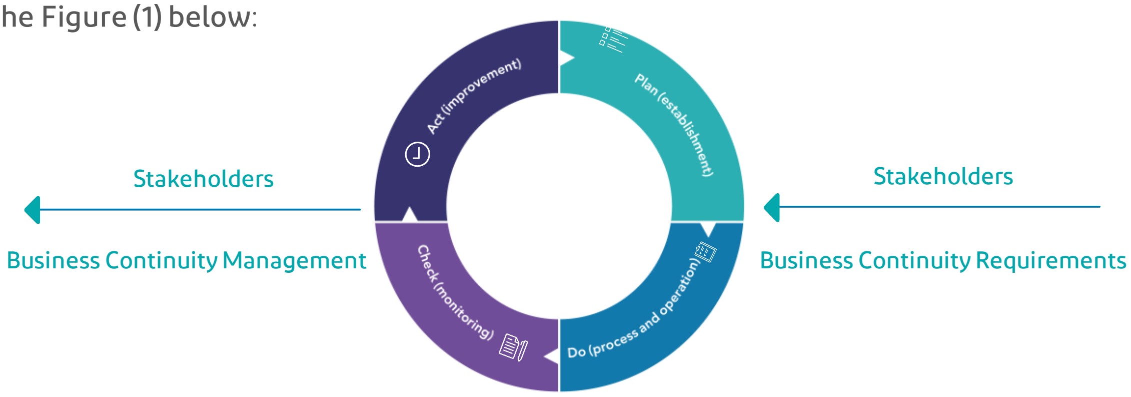

Stakeholders
Business Continuity Management
Act (improvement)
Plan (establishment)
Do (process and operation)
Check (monitoring)
Stakeholders
Business Continuity Requirements

Figure 1: Business continuity system sequence

4. Target Audience

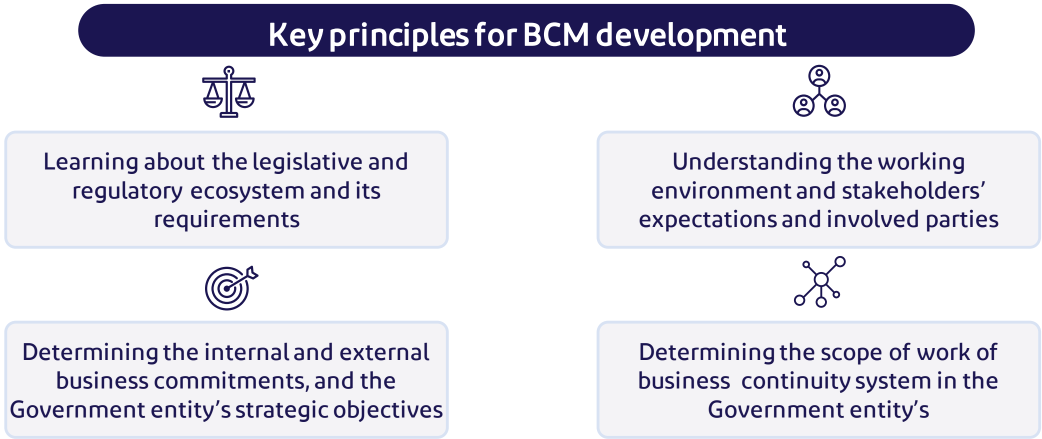
The recommendations contained in this document can be used by government entities that provide digital services and products and operators regardless of their type, size and nature. The applicability of the recommendations will depend on the entity's operating environment, level of complexity and number of its geographical locations.

5. Guideline Statement

5.1 Key principles for BCM development

In order to develop an effective and successful BCMS, it’s necessary to first understand the entity, the work environment and the operations processes, understand the needs and expectations of stakeholders, and define the scope of work of the BCMS. Then define the external and internal business obligations and suppliers, establish and develop a BCM policy, define the authorities , roles and responsibilities, then identify opportunities, risks and develop plans to deal with them, determine the strategic and operational objectives of the entity and develop plans to achieve them.

The basic principles of developing a BCMS includes identifying efficiencies, resources and effective ways to support the implementation of a business continuity system. It also includes risk assessment, business interruption impact analysis, incident response strategies and solutions, and operational recovery plans. It also involves monitoring, auditing, verification and performance appraisal. Finally, the processes of development, continuous improvement and correction.



Key principles for BCM development

Learning about the legislative and regulatory ecosystem and its requirements

Understanding the working environment and stakeholders’ expectations and involved parties

Determining the internal and external business commitments, and the Government entity’s strategic objectives

Determining the scope of work of business continuity system in the Government entity’s

Figure 2: Key Principles for Developing Business Continuity Management

5.2 Business Continuity Management System Methodology

Based on BCMS in Digital Government issued by DGA, the methodology of PLAN, DO, CHECK, and ACT (PDCA) must be followed, as shown in Figure (3) below:

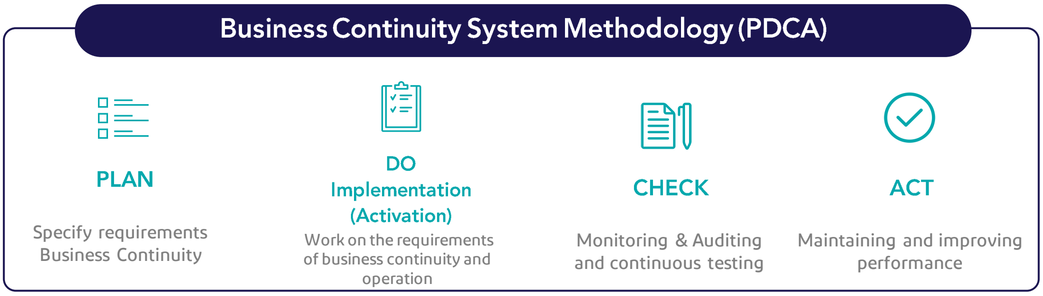

Business Continuity System Methodology (PDCA)
PLAN
Specify requirements Business Continuity
DO
Implementation (Activation)
Work on the requirements of business continuity and operation
CHECK
Monitoring & Auditing and continuous testing
ACT
Maintaining and improving performance

Figure 3: Business Continuity System methodology (PDCA)

5.2.1 Plan (Establishment)

BCM planning start with understanding the context of the Government entity's work, and the scope of its business continuity system based on the Government entity's internal and external business obligations related to its objectives and strategic vision to build business continuity policies and strategies, and clarifying its objectives, controls, procedures and roles and responsibilities of stakeholders, as their results support and develop the Government entity's policy and objectives. It should also be noted that the Business Continuity System objectives consistent with the Government entity's strategy, taking into account the context and organizational scope of the Government entity's , be shared with stakeholders within the system, and be continuously monitored and updated.

5.2.2 Do (Processes & Operation)

Based on the outputs of the Plan phase, the Do phase is then launched, which consists of:

- Analyze the impact of the digital processes, procedures and services interruption to determine the level of criticality according to a specific timeframe to prioritize. And determine the resources required for its continuity and internal and external dependencies.
- Build the necessary strategies and solutions to achieve the goals and objectives of restoring services and businesses and addressing the risks that may cause them to be disrupted.
- Identify associated risks to set recovery priorities, incident response and crisis management.
- Build business continuity or recovery plans based on a detailed analysis of the impact of the disruption of these processes or procedures.

5.2.3 Check (Monitoring & Review)

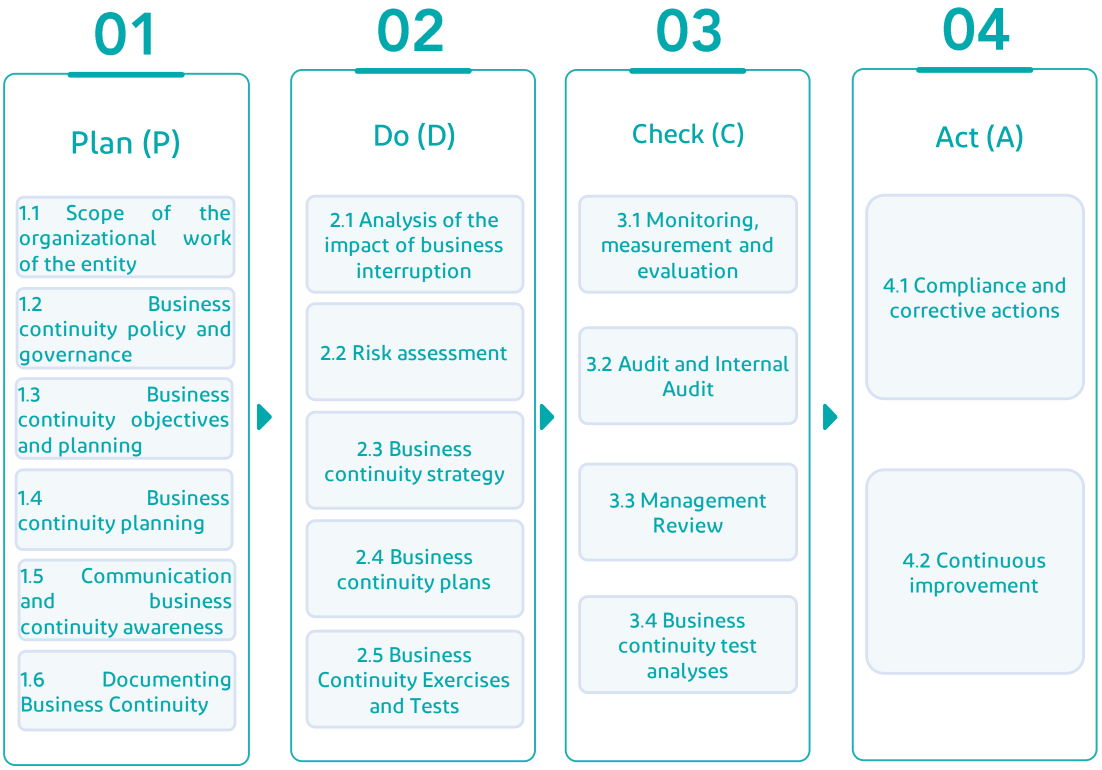
To ensure that the planned and implemented policies, plans, and strategies for business continuity are aligned with the Government entity's objectives and priority to restore its critical processes or procedures, the Business Continuity system subject to continuous verification through periodic review, continuous execution of tests and various scenarios to identify gaps and deficiencies. and training and awareness of those concerned with the Business Continuity Management system

5.2.4 Act (Improvement)

During this phase, gaps and shortcomings identified during the Check phase are corrected for the purpose of ensuring the effectiveness and alignment of the Government entity's business continuity system with the Government entity's operational and strategic objectives.

5.3 Business Continuity Management Framework

In order to build an effective and reliable BCM Framework, BCM processes identified and developed to implement the policies, objectives and controls. This is in line with the BCMS methodology "Plan, Do, Check, Act" (PDCA) and include business disruption impact analysis (BIA), risk assessment, business continuity strategy development and plans, and preparation and implementation of exercises and tests. In order to be guided by the most important sub-components to be implemented through the management cycle system, they can be projected as shown in Figure (4) below, so that these sub-components are implemented to achieve the objectives of the entire system and ensure its sustainability and compatibility with business variables, and its ability to adapt to all current and emerging events and crises to enable the entity to achieve its strategic objectives.



01

Plan (P)

- 1.1 Scope of the organizational work of the entity
- 1.2 Business continuity policy and governance
- 1.3 Business continuity objectives and planning
- 1.4 Business continuity planning
- 1.5 Communication and business continuity awareness
- 1.6 Documenting Business Continuity

02

Do (D)

- 2.1 Analysis of the impact of business interruption
- 2.2 Risk assessment
- 2.3 Business continuity strategy
- 2.4 Business continuity plans
- 2.5 Business Continuity Exercises and Tests

03

Check (C)

- 3.1 Monitoring, measurement and evaluation
- 3.2 Audit and Internal Audit
- 3.3 Management Review
- 3.4 Business continuity test analyses

04

Act (A)

- 4.1 Compliance and corrective actions
- 4.2 Continuous improvement

Figure 4: Business Continuity System Framework

5.3.1 Planning Phase

5.3.1.1 Government Entity regulatory scope

The first phase of the system starts with providing the necessary requirements and defining the Government entity's regulatory scope, including the context and regulatory scope of the Business Continuity System. This is achieved by defining the capabilities and the scope of the BCMS scope, taking into account the internal and external framework related to the Government entity's requirements, legal and legislative requirements as well as stakeholders.

This stage also involves identifying external and internal risks that may affect the government entity's services, processes, products, and procedures, and the Government entity's ability to handle risks in order to achieve its strategic objectives. Based on the Government entity's regulatory scope, key elements to be included in the scope of the BCS will be identified taking into account the geographical location of the entity, the size and nature of its business and the level of complexity. Departments, entities, procedures and processes to be included in the system are also identified. An illustrative example in Figure (5) below, showing the scope of business continuity and stakeholders within and outside the entity related to BCM.

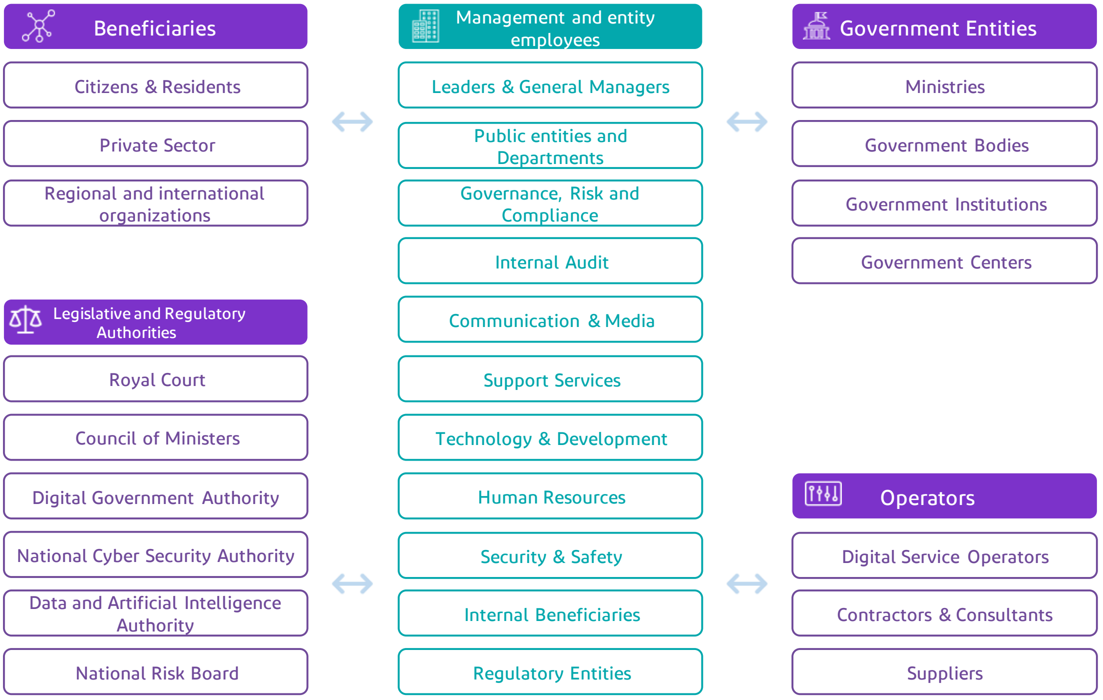

Beneficiaries
Citizens & Residents
Private Sector
Regional and international organizations
Legislative and Regulatory Authorities
Royal Court
Council of Ministers
Digital Government Authority
National Cyber Security Authority
Data and Artificial Intelligence Authority
National Risk Board
Management and entity employees
Leaders & General Managers
Public entities and Departments
Governance, Risk and Compliance
Internal Audit
Communication & Media
Support Services
Technology & Development
Human Resources
Security & Safety
Internal Beneficiaries
Regulatory Entities
Government Entities
Ministries
Government Bodies
Government Institutions
Government Centers
Operators
Digital Service Operators
Contractors & Consultants
Suppliers

Figure 5: General scope of business continuity

5.3.1.2 Business Continuity Policy and Governance:

By establishing business continuity policy and governance, it becomes easier to provide leadership and management direction to support BCM. During the development of the Business Continuity Policy and Governance, we should ensure that it is in line with the Government entity's work nature and support the development of business continuity objectives. This is in addition to supporting the commitment to the continuous development of key stakeholders and meeting the main requirements of the entity. As part of Business Continuity Governance, the entity identify the main committees and sub- committees of the Business Continuity System, roles, responsibilities and authorities of stakeholders and make sure to share them with them (for further information on the committees, roles, responsibilities and authorities, please refer to the appendix-9.1).

5.3.1.3 Planning for Business Continuity

Identifying the risks that addressed and the opportunities that must be exploited to ensure the achievement of the desired outcomes of the system and its continuous improvement. It is also necessary to identify procedures to address these risks, update the procedures and processes of the system, and evaluate the effectiveness of these procedures to achieve the desired results.

5.3.1.4 Business Continuity Objectives and Planning

Business continuity objectives, controls, processes and procedures are defined, considering what the system aspires to implement, what resources are needed, who is responsible, what is the target time, and how the assessment is carried out within a comprehensive framework to ensure business sustainability.

5.3.1.5 Business Continuity Communication and Awareness

Awareness of the system and its key elements, roles, responsibilities and authorities with various stakeholders. All stakeholders need to be fully informed and aware of the expected contributions from them to enhance the effectiveness of the system, the importance of the system, their tasks and responsibilities before, during and after crises or incidents of various kinds.

5.3.1.6 Business Continuity Documentation:

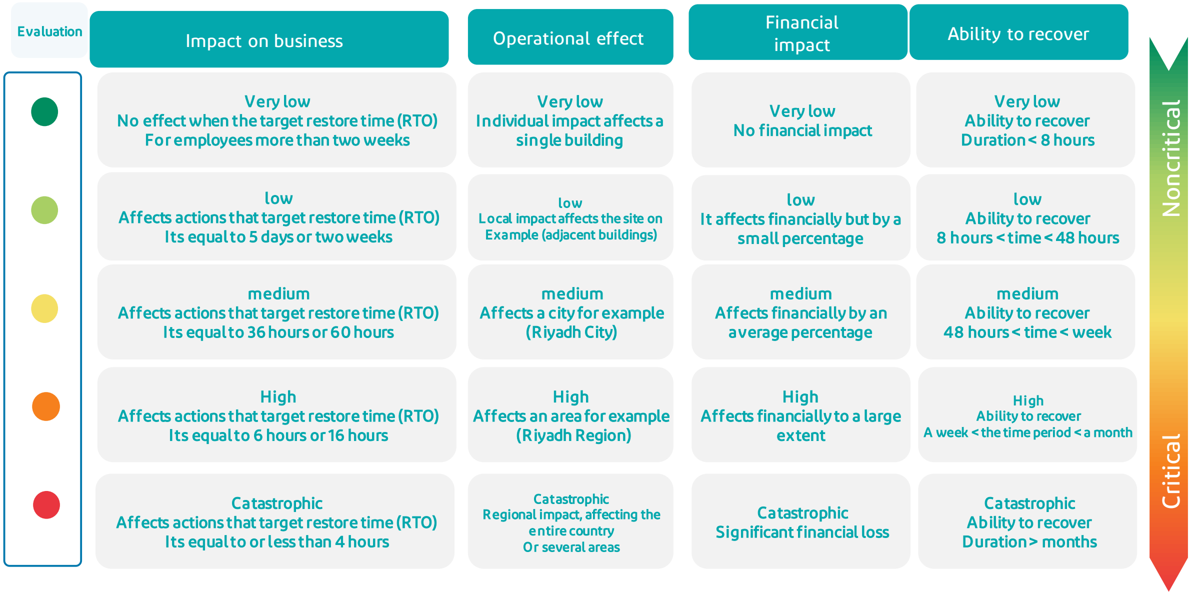
Documenting policies, standards and information supporting business continuity, ensuring that they are presented and approved by key stakeholders in accordance with the government entity's approved authority matrix, ensuring continuous awareness, and ensuring their availability to all stakeholders when needed.

5.3.2 Implementation and activation phase

5.3.2.1 Business Impact Analysis

The impact of business interruptions is analyzed through the process of analyzing business activities and the effects of their interruption due to possible accidents in order to determine the strategies to be followed in the event of interruptions/disturbances/accidents. Actions and activities are also prioritized based on their importance in the provision of products and services. The business interruption impact analysis phase is the cornerstone of the business continuity system and ensuring its effectiveness.

The phase of analyzing the impact of business interruption begins with the inventory of all internal and external procedures and processes of the entity and determine the procedures on which it depends and then analyze the impact of its interruption over time according to the matrix of the impact assessment of the interruption adopted for the entity below, with clarity of the critical processes or procedures of the entity, which helps to classify the platforms, as shown in Figure (6) below:

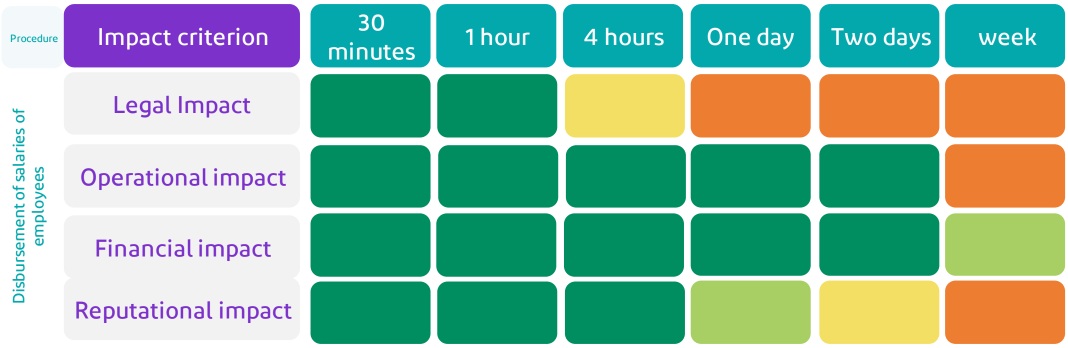

Noncritical
Critical

Evaluation	Impact on business	Operational effect	Financial impact	Ability to recover
●	Very low No effect when the target restore time (RTO) For employees more than two weeks	Very low Individual impact affects a single building	Very low No financial impact	Very low Ability to recover Duration < 8 hours
●	low Affects actions that target restore time (RTO) Its equal to 5 days or two weeks	low Local impact affects the site on Example (adjacent buildings)	low It affects financially but by a small percentage	low Ability to recover 8 hours < time < 48 hours
●	medium Affects actions that target restore time (RTO) Its equal to 36 hours or 60 hours	medium Affects a city for example (Riyadh City)	medium Affects financially by an average percentage	medium Ability to recover 48 hours < time < week
●	High Affects actions that target restore time (RTO) Its equal to 6 hours or 16 hours	High Affects an area for example (Riyadh Region)	High Affects financially to a large extent	High Ability to recover A week < the time period < a month
●	Catastrophic Affects actions that target restore time (RTO) Its equal to or less than 4 hours	Catastrophic Regional impact, affecting the entire country Or several areas	Catastrophic Significant financial loss	Catastrophic Ability to recover Duration > months

Figure 6: Example of a discontinuity impact assessment matrix

After the assessment, the entity has identified the critical actions and their required Recovery Time Objective (RTO), Recovery Point Objective (RPO), Maximum Tolerable Period of Disruption (MTPD), and Minimum Business Continuity Outage (MBCO) . The resources to be provided for the recovery of procedures such as human resources, equipment, technology systems, and facilities should also be identified. The timeline of the impact of the disruption is determined based on the sensitivity of the Government entity's work. For example, some entities consider that the impact of business disruption starts after half an hour due to its sensitivity. Therefore, it is preferable to start the timeline of the impact of the disruption from half an hour, while others start the impact after one or two days. Therefore, the impact assessment timeline also starts after one or two days.

For the purpose of illustrating the mechanism for classifying and evaluating procedures and the impact of their interruption on chronology, the example below shows how to classify and identify critical procedures by example in the evaluation: It can be argued that the Employee Salary Disbursement Procedure is critical given that the impact on at least one Business Impact Standard is considered high as per the impact assessment matrix in Figure (6), so the target recovery time of this procedure is considered two days, and the maximum time for its disruption is considered a week. As shown in Figure (7).



Procedure	Impact criterion	30 minutes	1 hour	4 hours	One day	Two days	week
Disbursement of salaries of employees	Legal Impact	🟩	🟩	🟨	🟧	🟧	🟧
	Operational impact	🟩	🟩	🟩	🟩	🟩	🟧
	Financial impact	🟩	🟩	🟩	🟩	🟩	🟢
	Reputational impact	🟩	🟩	🟩	🟢	🟨	🟧

Figure 7: Example of classification of actions

The Figure (8) below can be used to illustrate the difference between RTO, RPO, and MTPD.

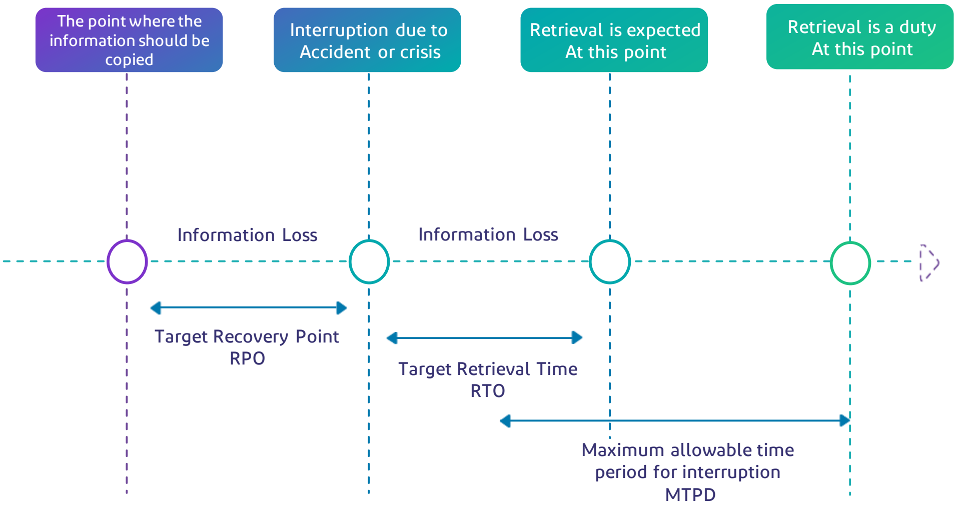

The point where the information should be copied
Interruption due to Accident or crisis
Retrieval is expected At this point
Retrieval is a duty At this point
Information Loss
Information Loss
Target Recovery Point RPO
Target Retrieval Time RTO
Maximum allowable time period for interruption MTPD

Figure 8: Recovery times

5.3.2.2 Risk Assessment

Risk assessment is key to building a successful and effective system because of the key role of this phase in identifying risks or threats to the Government entity's business continuity. The process also identifies the highest risks or threats, develops treatment plans and includes them in the business continuity strategy.

In addition to the above, the process of identifying and assessing risks and threats helps build crisis scenarios or incidents to simulate periodic business continuity tests and ensure that recovery teams, systems and equipment are ready to respond in the most effective way to restore operations within the planned recovery times.

Finally, the risk assessment process contributes to identifying a wide range of risks that threaten the entity and its likelihood. The assessment includes identifying risks, analyzing them, measuring them, and developing appropriate treatment plans for them.

To achieve the objectives of the risk assessment, we recommend following the three stages below:

• Risk identification:

The risk identification process is conducted to identify the resources that support the Government entity's critical and important operations, and to understand the impact of their disruption based on the results of the latest BIA.
Also, identifying incidents that may cause critical operations to fail and then classifying the likelihood of such incidents.

• Risk Analysis:

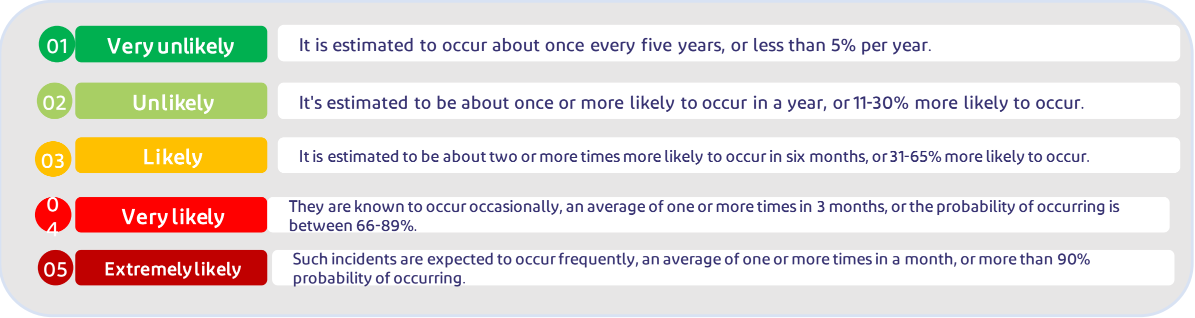
BCM oversees the implementation of the risk analysis phase, where, for example, HR, Safety, Security, IT and Cybersecurity Departments work together to analyze the risk of unavailability of resources supporting critical and important processes by analyzing the potential impact of the risk of an incident.
Several factors can be considered during the risk analysis process, which include likelihood of occurrence and impact.

The risk of disruption associated with each incident is calculated using impact and likelihood factors as shown in Figure (9) below.

For more details on the risk assessment stage, please refer to the "Risk Management Guideline for Digital Government" issued by DGA.

(These matrices can be modified and adapted in line with the Government entity's scope of work and internal risk assessment procedures).

It may only occur in exceptional circumstances, or it may occur once in two years, or it is less than 10% likely to occur.



01	Very unlikely	It is estimated to occur about once every five years, or less than 5% per year.
02	Unlikely	It's estimated to be about once or more likely to occur in a year, or 11-30% more likely to occur.
03	Likely	It is estimated to be about two or more times more likely to occur in six months, or 31-65% more likely to occur.
04	Very likely	They are known to occur occasionally, an average of one or more times in 3 months, or the probability of occurring is between 66-89%.
05	Extremely likely	Such incidents are expected to occur frequently, an average of one or more times in a month, or more than 90% probability of occurring.

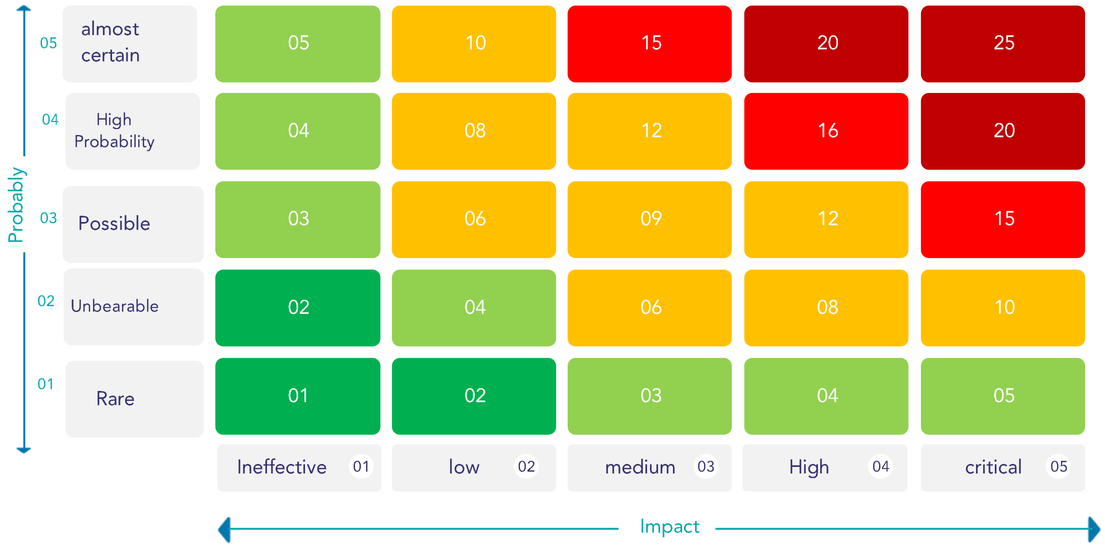
Figure 9: Example of risk probability assessment

• Risk Assessment:

This phase is carried out by the BCM to identify the risk incidents that are rated above the Government entity's thresholds and in accordance with the Government entity's business continuity and risk tolerance objectives, which requires solutions to reduce the likelihood of occurrence and its impact, and these risks should be addressed when developing the business continuity strategy.

Based on the Risk Impact Assessment and Risk Likelihood Assessment matrices, the risk of disruption is calculated as*: (Inherent risk = impact x likelihood)*

According to the heat map of the risks shown in Figure (10) below, risks are categorized based on the Government entity's risk acceptance level, where the risk of low and medium disruption is accepted or managed, but the risk of high disruption cannot be accepted. Preventive controls identified in the Business Continuity Strategy, where preventive controls aim to reduce the likelihood or impact of the risk and thus reduce the risk of disruption to the Government entity's operations and resources.



Probably						
05	almost certain	05	10	15	20	25
04	High Probability	04	08	12	16	20
03	Possible	03	06	09	12	15
02	Unbearable	02	04	06	08	10
01	Rare	01	02	03	04	05
		Ineffective 01	low 02	medium 03	High 04	critical 05

Figure 10: Risk assessment heat map example

Risks can be divided into several groups based on the results of the assessment according to the type of resources that support critical processes as shown below:

- Lack of availability of documents
- Lack Third Parties
- Lack of availability of information systems
- Unavailability of persons or employees
- Lack of facilities

5.3.2.3 Business Continuity Strategy

Based on the outputs of the BIA and Risk and Threat Assessment for the government entity's business, the entity build the Business Continuity Strategy, to be aligned with the Government entity's strategy which sets out solutions to be implemented to increase the efficiency of the government entity's business continuity or its ability to recover its business according to the target times. The strategy also include details of the resources needed to implement these solutions, which are not limited to the financial aspect, but extend to human resources, equipment, systems, facilities and other resources.

5.3.2.4 Business Continuity Plans

As discussed in advance, the Business Impact Analysis (BIA) stage is the cornerstone of the business continuity system, through which procedures or processes are analyzed in the entity, the critical ones are identified, and recovery priorities are set. Accordingly, business continuity plans are developed, including the following:

- Emergency Management Plan:

Focuses more on emergencies and how to deal with them to ensure the Government entity's business continuity and protect the lives of its employees.

- Crisis Management Plan:

Mainly focused on the crises that the entity can face and how to deal with them holistically. The plan includes the Crisis Management Team members, their tasks and responsibilities, recovery plans activation indicators and response teams. The plan also includes stakeholders and external entities to be informed when a crisis occurs.

- Business Recovery Plans:

These focus primarily on plans to restore the business of a department or entity that has critical procedures. At least one plan is developed for each entity or department that has critical procedures, and a copy of the plan made available to all recovery teams in the department or entity. The business recovery plan include all critical procedures and recovery times, the internal communication system (call tree) in the department or entity during incidents of disruption, and all human and technical resources and equipment to be provided for the recovery of services.

Such plans clarify all internal and external approvals for such procedures or services. If there are approvals for external entities to implement these procedures, the methods and information of communication with these entities included.

- Technical Disaster Recovery Plans:

These plans focus directly on the technical systems that support the continuity of critical procedures in the entity, and the entity must ensure that technical disaster recovery plans are developed in line with the requirements of recovery of critical procedures. If there are gaps between the technical capabilities to recover services and business requirements, we must ensure that these gaps are included in the business continuity strategy with proposed solutions that need to be implemented to overcome these gaps.

- Media Response Plan:

Focuses on internal and external communication plans and identifies stakeholders in communication during the crisis or incident while setting the messages to be announced, the spokesperson, communication channels, and dealing with risk scenarios that affect the Government entity's reputation and handling them properly. The plans also include monitoring social media developments regarding the incident and dealing with them if necessary.

The Business Continuity Plans (BCPs) aim to ensure that response teams are prepared to manage disruption-causing incidents by documenting the response structure and coordinating communications. Also, the plans ensure that guidelines and instructions are available by documenting them to serve as a reference for the response team in case of breakdowns and failures.

- Crisis Management Team:

The crisis management team starts under the direction of the head of the entity to assess the potential impact on the Government entity's critical resources and operations, and accordingly decide to activate the Business Continuity Plan and determine the expected time for recovery. The crisis teams will assess the impacts, set priorities, coordinate and assist other teams with the necessary actions.

- Business Recovery Team:

Business recovery teams work to maintain the Government entity's business continuity and the critical government services, and the recovery of disrupted services within specified periods not exceeding MTD. The teams also follow the guidelines and report to the crisis management team.

- Incident Response Team:

The Incident Response Team acts immediately in the event of an incident to ensure the safety of employees, save the Government entity's assets, follow directions and report to the crisis management team. The incident response team consists of security and safety department and building management.

• Disaster Recovery Team and Cyber Incident Response Team:

The IT Disaster Response Team ensure the business continuity of the technical systems and work to return to normal. The Cyber Incident Response Team will deal with security incidents and cyber threats, identify risks and try to reduce the impacts, . In addition, follow the guidelines and report to the crisis management team. And document the incidents to avoid them in the future

• Media and Communication Team:

The Communication and Media Team work on internal and external communication to inform stakeholders during the incident until its fully recovered, in addition, follow the guidelines and report to the crisis management team.

For guidance, an example of an incident response structure is shown in Figure (11) below:

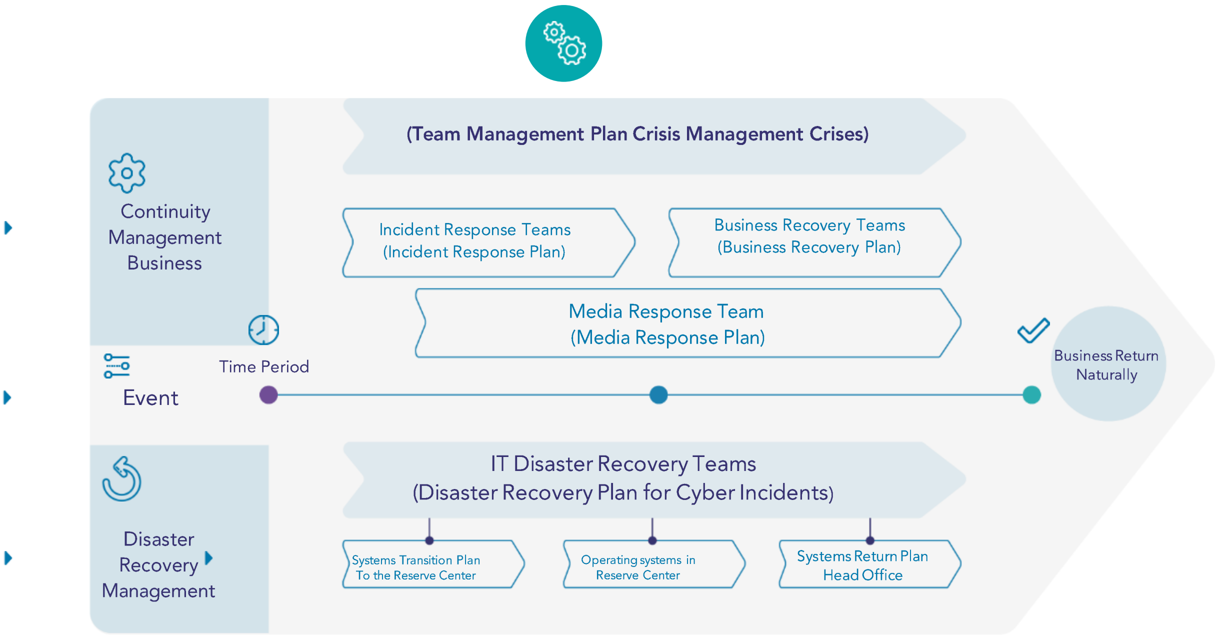

(Team Management Plan Crisis Management Crises)
Continuity Management Business
Incident Response Teams (Incident Response Plan)
Business Recovery Teams (Business Recovery Plan)
Media Response Team (Media Response Plan)
Time Period
Event
Business Return Naturally
IT Disaster Recovery Teams (Disaster Recovery Plan for Cyber Incidents)
Disaster Recovery Management
Systems Transition Plan To the Reserve Center
Operating systems in Reserve Center
Systems Return Plan Head Office

Figure 11: Example of the Incident Response Structure

5.3.2.5 Business Continuity Drills and Tests:

Training and awareness developed to explain the Business Continuity Plan to all stakeholders internally and externally, in preparation for the implementation of the annual exercise and testing system to verify the effectiveness of the Business Continuity Plans and their solutions. Drills and tests are key to testing all forms of Business Continuity Plans. Tests should not be focused on specific plans but should cover all BCPs and recovery teams. It is also advisable to hold several tests annually with different scenarios according to the risk and threat register surrounding the entity.

5.3.2.6 Management review

Review the BCMS and procedures for business continuity continuously in the government entity's, to ensure alignment with the directions of top management and the strategic objectives of the government entity's.

5.3.3 Monitoring and Review Phase

5.3.3.1 Monitoring, Measurement and Evaluation:

It is essential to assess the suitability, efficiency, and effectiveness of the BC system's capacity and performance at least once annually by building and continuously assessing performance indicators for development and improvement.

5.3.3.2 Internal Audit and Review:

The review and audit process carried out by reviewing compliance reports, internal audit and external entities' reports, as well as the reports of that have the right to review business continuity controls and disaster recovery. These gaps taken into consideration.

5.3.3.3 Management review

Review by the top management of the system on an ongoing basis to ensure alignment with the directions of the top management and the government entity's strategic objectives.

5.3.3.4 Analysis of business continuity tests

Business continuity plan trainings and tests analyzed to ensure their effectiveness and to improve them. The official post-exercise report should be documented, including the executive summary, the exercise scenario, the type of plan and the date of its implementation, the teams involved in the exercise or test, and the stages of the exercise or test.

5.3.4 Maintenance and Improvement Phase

5.3.4.1 Compliance and Corrective Actions:

Based on the gaps and deficiencies identified in the review and evaluation phase, the Business Continuity team address these gaps by implementing corrective measures to improve the efficiency of business continuity in the entity. The BCMS reviewed once annually by an internal or external qualified and experienced auditor.

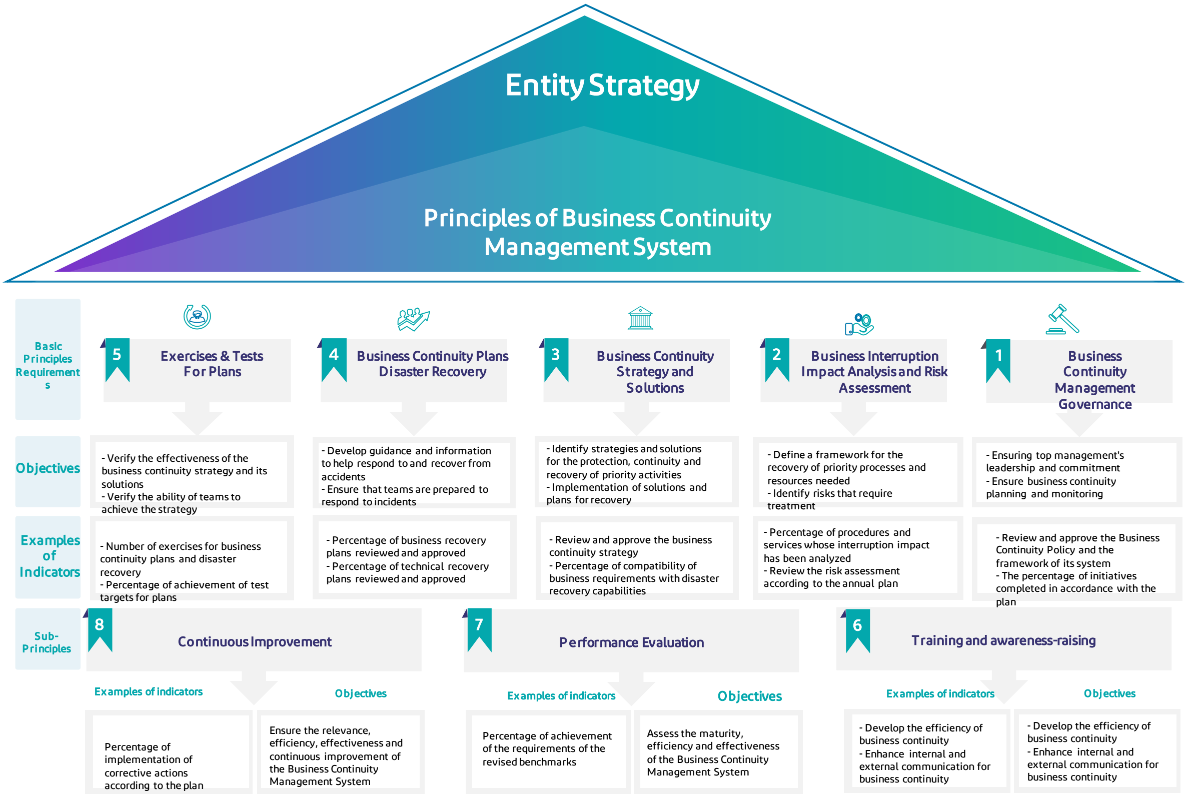
5.3.4.2 Continuous Improvement:

The results of the internal and external audit escalated to top management and the Business Continuity Steering/Supervisory Committee for review, to ensure that corrective actions are taken. The suitability, efficiency, and effectiveness of the BC system continuously improved to achieve the targeted outcomes.

5.4 Business Continuity Performance Indicators

Business continuity performance indicators are a key factor for the success of the BCMS and the achievement of its objectives.

It must be directly linked to the principles and strategy of the entity in order to enable sustainability and the ability to implement it properly. An example of the binding process and its mechanism is shown in Figure (12) below.



Basic Principles Requirements	5 Exercises & Tests For Plans	4 Business Continuity Plans Disaster Recovery	3 Business Continuity Strategy and Solutions	2 Business Interruption Impact Analysis and Risk Assessment	1 Business Continuity Management Governance
Objectives	- Verify the effectiveness of the business continuity strategy and its solutions - Verify the ability of teams to achieve the strategy	- Develop guidance and information to help respond to and recover from accidents - Ensure that teams are prepared to respond to incidents	- Identify strategies and solutions for the protection, continuity and recovery of priority activities - Implementation of solutions and plans for recovery	- Define a framework for the recovery of priority processes and resources needed - Identify risks that require treatment	- Ensuring top management's leadership and commitment - Ensure business continuity planning and monitoring
Examples of Indicators	- Number of exercises for business continuity plans and disaster recovery - Percentage of achievement of test targets for plans	- Percentage of business recovery plans reviewed and approved - Percentage of technical recovery plans reviewed and approved	- Review and approve the business continuity strategy - Percentage of compatibility of business requirements with disaster recovery capabilities	- Percentage of procedures and services whose interruption impact has been analyzed - Review the risk assessment according to the annual plan	- Review and approve the Business Continuity Policy and the framework of its system - The percentage of initiatives completed in accordance with the plan

Sub-Principles	Examples of indicators	Objectives
8 Continuous Improvement	Percentage of implementation of corrective actions according to the plan	Ensure the relevance, efficiency, effectiveness and continuous improvement of the Business Continuity Management System
7 Performance Evaluation	Percentage of achievement of the requirements of the revised benchmarks	Assess the maturity, efficiency and effectiveness of the Business Continuity Management System
6 Training and awareness-raising	- Develop the efficiency of business continuity - Enhance internal and external communication for business continuity	- Develop the efficiency of business continuity - Enhance internal and external communication for business continuity

Figure 12: Example of linking business continuity indicators to principles and entity strategy

5.5 Business Continuity Success Factors

In order to enhance the role of BCM in the entity and ensure that it achieves the desired objectives, here is a list of enablers:

- Independence of business continuity from the executive management (Three-Lines Model - Figure 11 in the appendix).
- Entity leaders are supportive, engaged and committed to the implementation of the BCM strategy and framework.
- Establish a committee that's composed of BCM leadership team that will contribute to pointing out the Government entity's direction and support adopting BCM principles in the entity.
- Ensure a comprehensive understanding of the objectives, activities and related risks and the mechanism to address and mitigate them.
- Understanding internal and external risks that may lead to business interruption, analysis, evaluation and proactive management by preventing threats that may hinder the achievement of objectives and dealing with them if they occur.
- Identifying and managing shared risks with different internal and external parties and managing them in an integrated and systematic way.
- Following a gradual approach in implementing the system, initially based on a simplified approach that could be developed according to the experience and knowledge acquired.
- Aligning the BCM approach with the Risk Management approach and ensuring integration between them.
- Including BCM into the Government entity's key management processes, including the process of strategic planning, goal setting and achievement, and implementation of initiatives and projects.
- Focusing on implementing the methodology of identifying, analyzing and evaluating risks and not only the current problems facing the departments in the entity.
- Providing adequate resources to establish and maintain BCM functions.
- Balanced investment in institutional infrastructure to increase the Government entity's preparedness to face disasters and accelerate recovery.
- Raising awareness of the importance of BCM through workshops, exercises and tests for internal awareness plans and campaigns.

6. Table of Definitions

The following terms and expressions - wherever they appear in this document - shall have the meanings indicated on the opposite side of each of them, unless the context requires otherwise

Term	Definition
DGA	Digital Government Authority.
Government Entities	Ministries, authorities, public institutions, councils, national centers including any additional form of a public entity.
Business Continuity (BC)	The ability of the entity to continue its prioritized activities at predetermined levels after the occurrence of a disruptive incident
Business Continuity Strategy (BC Strategy)	The method of an entity to plan in order to recover and continue after a disruptive event.
Business Continuity Management System (BCMS)	A part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.
Business Continuity Plan (BCP)	Documented information that guides an entity to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.
Organizational Flexibility	The organization's ability to assimilate and adapt in a changing environment to enable it to achieve its goals, survive and thrive.
Information Technology (IT) Disaster Recovery (DR)	Digital technology to recover its critical systems to an acceptable level within a predetermined period of time following a disruption. The ability of the IT DR elements of an entity including all
Impact	The impact is the consequence of the risk if it's materialized.
Event	Any event that has a consequence that may affect the achievement of objectives, negatively or positively.
Resources	Resources include information, skills, people, technology, suppliers, assets and premises, which are obtained and used by an entity to achieve its organizational goals and objectives.
Stakeholders	Parties and entities that affect and are affected by decisions, directions, procedures, objectives, policies and initiatives of the digital government and share some of their interests and outputs and are affected by any change that occurs in them..

Term	Definition
Target Recovery Time (RTO)	Period of time following an incident within which a product and service or an activity or resources are recovered.
Recovery Point Objective (RPO)	Point to which information used by an activity is restored to enable the activity to operate on resumption.
Maximum Tolerable Period of Disruption (MTPD)	Time it would take for adverse impacts, which might arise as a result of not providing a product, service or performing an activity, to become unacceptable.
Minimum Business Continuity Objectives (MBCO)	Minimal level for a product or service, which are considered appropriate for the entity to still accomplish its organizational goals after disruption.
Business Impact Analysis (BIA)	Process for analyzing business activities and the impacts over time of a disruption on the entity.
The Crisis	An abnormal and unstable situation that threatens the strategic objectives of the entity, their reputation or survival.
Compliance	Extent to which requirements are fulfilled.
Continuous Improvement	Recurring activity to enhance performance of the BCMS.
Disruption	An incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an entity's objectives.
Exercises	Activity in which the business continuity plans are rehearsed in part or whole to ensure that the plans contain the appropriate information and produce the desired results when activated.
Internal Audit	A compliance review against BCM standard or policy requirements.
Management Review	Management's review for a certain situation or reconsideration of a certain topics.

Term	Definition
Media Response Plan (MRP)	A plan providing details of the entity's media response following an incident, including a communications strategy.
Remote Working	A work system in which the worker performs his job duties for the benefit of his employer, and under its supervision, in a place other than the usual workplace at the headquarters of his workplace inside the Kingdom, whether the work is full or part time, using means of communication and information technology.
Performance Appraisal	Used to check how well roles and responsibilities are being undertaken.
Prioritized Activities	Activity to which urgency is given in order to avoid unacceptable impacts to the business during a disruption.
Process	A set of interrelated or interacting activities which transforms inputs into outputs.
Recovery	Documented processes to restore and return business activities from the temporary measures adopted during and after a disruption.
Test	This is an activity or action that is undertaken to gauge the capabilities and effectiveness of a strategy or plan against a predetermined criteria or benchmark. (This shall include a pass/fail element)
Top Management	All those responsible for making key decisions within the entity.
Training	This activity is more formalized compared to awareness. It purports to build skills and competencies to increase the performance of staff regarding a specific role or responsibility
Enterprise Risk Management (ERM)	Risk management involves understanding, analyzing, and addressing risk to make sure organizations achieve their objectives.
Risk	Events that might occur and effect the achievement of the entity objectives.
Risk Tolerance (RT)	Reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achiev . (COSO ERM)
Risk Assessment	The process of identifying, analyzing and evaluating the risks that might impact the achievements of objectives.

7. Table of Abbreviations

Abbreviations	Description
RTO	Recovery Time Objective
RPO	Recovery Point Objective
MTPD	Maximum Tolerable Period of Disruption
MBCO	Minimum Business Continuity Objective
BIA	Business Impact Analysis

8. Appendix

8.1 Roles and responsibilities

Roles and responsibilities need to be defined, providing the opportunity to achieve better results in terms of time, cost and efficiency. The definition of roles and responsibilities also illustrates the expectations of third parties from the system. The governance model describes the responsibilities and authorities in the Business Continuity System, which was organized into three categories, starting with Governance and Accountability, Implementation and Operation, and then Incident Response. Below is a simple explanation of the key responsibilities of the stakeholders within the entity towards the BCMS.

8.1.1 Head of Entity

The head of the entity is responsible for overseeing and adhering to governance and risk management and approving acceptable maximum risk levels. The head of the entity also assumes overall responsibility for business continuity including approval of the Business Continuity Policy and assign the BCM Sponsor.

8.1.2 Director of Business Continuity Management

Responsibilities of the Sponsor of the Business Continuity System:

- Ensure the effective implementation of the business continuity policy, strategy and framework and provide the necessary materials, including budget allocation.
- Participate in awareness activities on the importance of business continuity such as hypotheses, exercises and training workshops.
- Continuous improvement of business continuity management and dissemination of its importance.
- Incident response management and business continuity plans.
- Represent business continuity in the management reviews of the Business Continuity Management System.

8.1.3 BCM Steering Committee

The BCM Steering Committee is responsible for monitoring the implementation of BCM programs; its responsibilities include:

- Monitoring the BCMS and implementing its principles.
- Approving the annual training system and awareness programs.
- Approving the process recovery timeline and identifying risks that require mitigation.
- Approving the BCM framework.
- Implementing the initiatives plan, monitor business continuity objectives, and studying and approving proposed changes.

8.1.4 Governance, Risk and Compliance Department

The Governance, Risk and Compliance Department is responsible for overseeing the risk management policy and developing the governance and compliance framework.

8.1.5 Internal Audit Department

The Internal Audit Department is responsible for assessing the BCMS compliance by the following:

- Principles, objectives and controls of the Business Continuity Policy
- Benchmarks such as: requirements of ISO 22301:2019
- The Business Continuity Policy and its alignment with relevant policies

8.1.6 Business Continuity Management Department

The department heads responsibility is to:

- Implement the Business Continuity Policy and Framework, ensure the integration of tasks within departments and ensure the availability of the resources.
- Provide support, time and resources to business continuity leaders.
- Approve, update and archive business continuity plans and ensure that plans are executed correctly.
- Agree on a timeframe for disaster recovery and ensure corrective measures are taken.

8.1.7 Business Continuity Management

The BCM Department's job is to:

- Ensure the development and implementation of the Business Continuity Policy and Framework, review and publish the latest versions of the policy and framework.
- Prepare the annual initiatives and objectives plan of the business continuity system.
- Ensure that corrective actions are implemented to address incidents and develop annual drill programs to check the roles of the responsible team.
- Develop and review business continuity strategy and solutions in collaboration with IT, HR, Security and Safety.
- Conduct risk assessment workshops and disruption impact workshops.

8.1.8 Security, Safety and Facilities Management

Security and Safety Department Responsibilities:

- Facilitate and participate in risk assessment workshops and implement preventive controls.
- Maintain security and emergency plans for buildings by enhancing evacuation practices and implementing workplace recovery solutions or providing alternative facilities.
- Promote and maintain epidemiological plan practice.

8.1.9 Information Technology Management

Information Technology Department is responsible for:

- Developing and updating the disaster and crisis recovery plan
- Participate in workshops to assess risks in addition to implementing technical preventive controls.
- Enhance and maintain technical services continuity and recovery plans exercises.
- Ensure that workplace restoration solutions are implemented in alternative facilities and telecommuting.

8.1.10 Cybersecurity Management

The responsibilities of the Cybersecurity Department include:

- Participation in risk assessment workshops and implementation of preventive controls.
- Develop, update and enhance response plans to cyber incidents.
- Conduct annual assessments and exercises to determine the adequacy of security controls.

8.1.11 Human Resource Management

The Human Resources Department works on:

- Participate in workshops to assess the risks of unavailability of employees to implement preventive controls.
- Provide support and contribute to epidemiological plan tests.
- Maintain records of business continuity competencies and qualifications.

8.1.12 Supplier/Third Party Management

Responsibilities of Supplier/Third Party Management:

- Classify the performance according to service level agreements.
- Determine the target recovery time and target recovery point in the contract.
- Understand supplier business continuity management system.

8.1.13 All departments of the entity

Responsibilities of all departments of the entity:

- Ensure the nomination of entrepreneurs for business continuity.
- Participate in disaster recovery and maintenance exercises.
- Participate in workshops in analyzing the impact of business interruptions.

8.2. Integration between BCM and “Three Lines Modell”

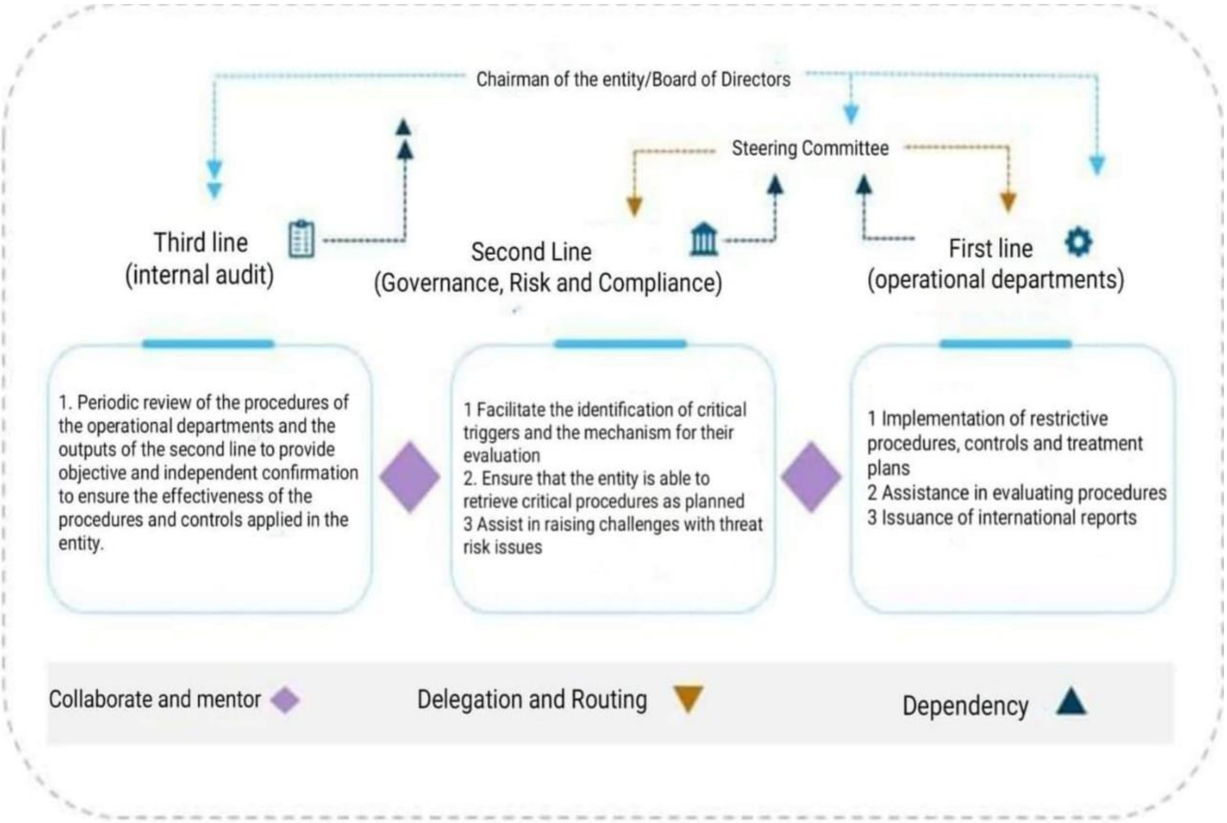

Chairman of the entity/Board of Directors
Steering Committee
Third line
(internal audit)
Second Line
(Governance, Risk and Compliance)
First line
(operational departments)
1. Periodic review of the procedures of the operational departments and the outputs of the second line to provide objective and independent confirmation to ensure the effectiveness of the procedures and controls applied in the entity.
1 Facilitate the identification of critical triggers and the mechanism for their evaluation
2. Ensure that the entity is able to retrieve critical procedures as planned
3 Assist in raising challenges with threat risk issues
1 Implementation of restrictive procedures, controls and treatment plans
2 Assistance in evaluating procedures
3 Issuance of international reports
Collaborate and mentor ◆
Delegation and Routing ▼
Dependency ▲

Figure 13: Three Lines Model

BCM is classified as a second line model across entities and operates in parallel with the Governance, Risk and Compliance function in the same line. Their work largely intersects with the aim of providing a strong ”second line” supporting the “first line” represented by the operational departments and the “third line” represented by the Internal Audit Function. (Figure 13) shows the Three-Lines Model in the government entity.

BCM relies on Risk Management to identify the approved risk appetite levels within the government entity’s and adopt the risk assessment matrices approved and applied within the government entity’s . BCM, on the other hand, provides an integrated risk register that can be provided to Risk Management in relation to threats that could disrupt the government entity’s business while providing plans to address or mitigate these risks.

BCM also relies on Governance and Compliance Department to support in defining the roles and responsibilities of all parties involved in business continuity and identify the authority to activate business continuity plans in case of crisis or incidents. Also, the Governance and Compliance Function will support in developing policies and governance for the BC system and setting up the necessary committees to support BCM.

In terms of integration with the third line, the Business Continuity Department, in alignment with the Risk Department, supports the internal audit by providing a risk register, which would help in building the annual internal audit plan and prioritizing the annual review of the Government entity's business and the periodicity of reviews.

Business continuity also supports the Internal Audit Department by reviewing business continuity procedures, plans, and strategies and identifying shortcomings or gaps to support the continuous improvement process and applying best international practices for business continuity management in the government entity's .

8.3. Examples of the application of Business Continuity System standards

All forms below are general information for guidance only, and government entities should rely on facts and specific operating conditions and surroundings. Digital Government Authority does not make any declarations or guarantees, or obligate government entities to use these forms.

- Example of the roles and responsibilities standard of business continuity employees:

Standard Number	Standard
5-103-01	Appointing Business Continuity manager who has sufficient competencies and powers to manage the BCMS.

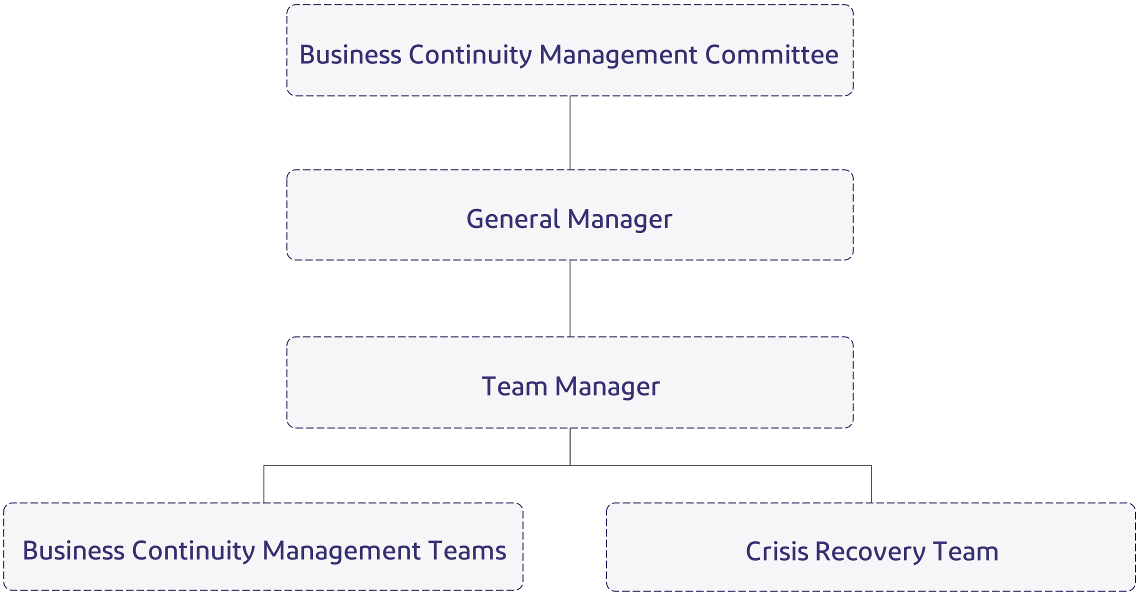
Some examples of the roles and responsibilities of business continuity employees:

- Develop and maintain a business recovery plan and procedures.
- Review existing plans and protocols, if any.
- Ensure that the Business Continuity Management System is implemented in accordance with the directives of top management included in the Business Continuity Policy.
- Conduct risk assessment for various departments and analyze the impact of possible business interruption of critical services in the entity.
- Collaborate with IT staff and relevant departments to develop and implement best practices for data protection and systems and their recovery in the event of disasters and crises.
- Supervise the implementation of exercises to practice the business continuity plan.
- Perform other duties related to the employee.

- Example of a business continuity management standard:

Standard Number	Standard
5-103-10.01	Business Continuity Management Structure and Resources

- Example of a business continuity management structure:



Business Continuity Management Committee
General Manager
Team Manager
Business Continuity Management Teams
Crisis Recovery Team

- Example of a training and awareness plan:

Standard Number	Standard
5-103-10.02	Training & Awareness

- Example of a training and awareness plan:

Business Continuity Awareness	Business Continuity Training
Launching business continuity awareness campaigns through the following channels, for example: • E-mail address • Newsletter • Business Continuity Awareness Week • Internal location and signage **Business continuity awareness can also be achieved through workshops and meetings through the following channels and methods:** • Workshops on specific topics for the purpose of awareness or training. • Brainstorming meetings to discuss specific topics for the purpose of awareness or training.	**Ensure understanding of the training requirements in the entity through cooperation with the Human Resources Department, and work to integrate the training of employees on multiple skills and succession planning, and the types of training:** • Intensive professional courses through a certified instructor. • Specialized courses in specific topics through the Learning Management System.

- Example of business interruption impact standards:

Standard Number	Standard
5-103-10.03	Business interruption impact analysis

- Example of business interruption impact analysis:

#	Department Activity	Activity Description	The time when the activity is important	Impact class
1	Employee salary disbursement	Receive the list of employees through the Human Resources Department. And send the Excel file to the bank via email monthly	Monthly	Impact on customers

Effect in case of interruption of activity					Maximum allowable time period for interruption	Level of importance of the activity	Target Retrieval Time
1-30 minutes	1 - 4 hours	4 - 8 hours	1 - 2 days	Two Days - Week			
Low	Low	Low	Medium	High	A week	High	Two weeks

- Example of a risk and threat assessment:

Standard Number	Standard
5-103-10.04	Risk and threat assessment

- Example of a risk and threat assessment matrix:

General Department	Department	Sector	Risk Status	Risk Number	Example Number
Human Resources Management	Human Resource s	Strategy & Partnerships	Active	001	1

Risk Classification	Risk Discription	Source of Risk Registration	Date of Risk Registration	Risk Causes
Operational Risk	Lack of job description and clarity of roles and responsibilities, which leads to overlapping tasks and affects the productivity of the employee and the quality of work	Human Resourc es Department	1/1/2022	1. Absence of policies and procedures 2. Lack of competencies and human resources 3. Lack of documentation of roles, responsibilities, job descriptions and management structure

- Example of disaster recovery methodology (IT DR) :

Standard Number	Standard
5-103-10.07	Disaster Recovery (IT DR)

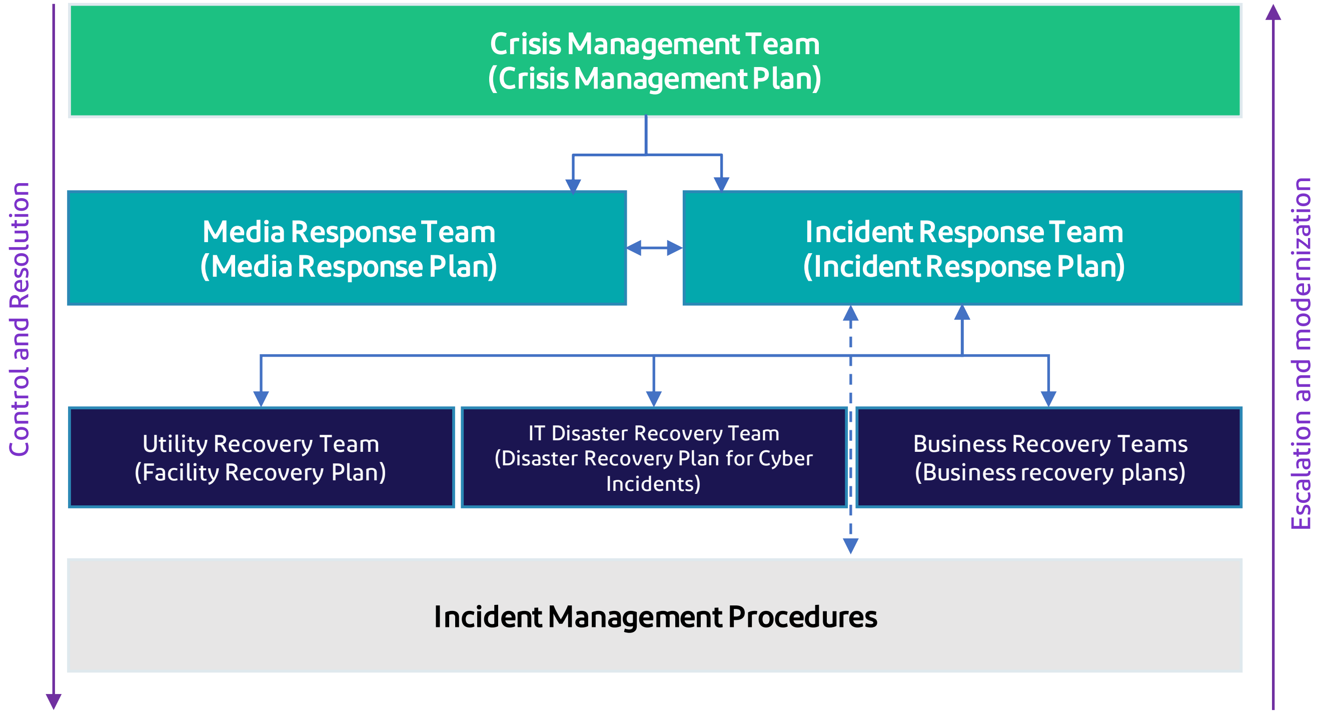
- Example of stages of disaster recovery methodology (IT DR) :

Stage	Description
1- Preparation	A plan must be developed to prevent and respond to security incidents.
2- Detection and analysis	Determine whether the security incident occurred, its severity, and type
3- Containment and eradication	Stop the effects of the accident before it causes further damage
4- Recovery after the incident	A meeting of lessons learned involving all parties concerned should be mandatory after a major accident and desirable after less serious incidents in order to deal better with incidents.

- Example of incident response plans standards:

Standard Number	Standard
5-103-10.08	Response Plans Structure

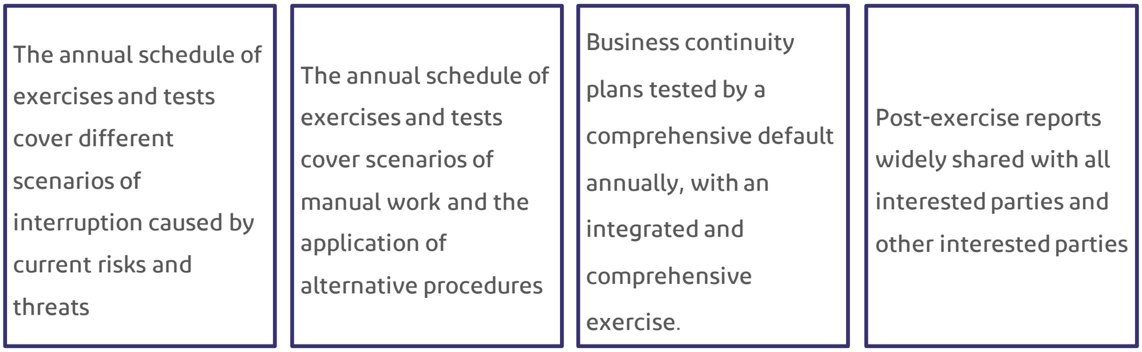
- Example of incident response plans structure:



- Example of the life cycle of exercises and tests standards:

Standard Number	Standard
5-103-10.09	exercises and tests

- Example of a life cycle of exercises and tests:



The annual schedule of exercises and tests cover different scenarios of interruption caused by current risks and threats

The annual schedule of exercises and tests cover scenarios of manual work and the application of alternative procedures

Business continuity plans tested by a comprehensive default annually, with an integrated and comprehensive exercise.

Post-exercise reports widely shared with all interested parties and other interested parties

- Example of the types of tests:

Live

Default

Simulation

List of Figures

هيئة الحكومة الرقمية
Digital Government Authority

DGA.GOV.SA