Digital Government Authority
هيئة الحكومة الرقمية

Controls

of Risk Management and Business Continuity for Digital Government

September 2025

Document Type: Controls

Document Classification: Public

Issue No: 4.0

Document No: DGA-1-2-5-107

Contents

1. Preamble

Regarding Cabinet Resolution No. (418) dated 25/7/1442 AH, which approved the regulation of the Digital Government Authority (DGA), it stipulates that DGA is the competent authority for all matters related to digital government and serves as the national reference in this domain. Pursuant to its mandate, DGA shall **"develop the technical standards for digital transformation models in government sectors and monitor compliance with them in coordination with the relevant authorities."**

In line with the aforementioned, DGA strives to enhance digital performance across government agency, improve the quality of services delivered, and elevate the end-user experience, all in alignment with the ambitious goals of Vision 2030.

DGA paves the way for government agency to deliver high-quality, efficient digital government services that drive investment returns, strengthen the value of the national economy, and enable the measurement of government agency' performance and capabilities in the digital government domain.

From this perspective, DGA issued the fourth version of the "Controls of Risk Management and Business Continuity for Digital Government" in accordance with the regulations issued by the competent authorities. DGA remains responsible for regularly updating and reviewing this document to reflect evolving requirements.

2. Introduction

These controls form part of the regulatory framework for digital government, which contributes to raising the maturity level of digital government services and strengthening agency' ability and flexibility to identify risks and threats proactively. This is achieved through the establishment of a continuously improving risk management system and the development of business continuity plans. Such plans address response and recovery from service disruptions, aiming to minimize negative impacts and ensure the sustainability of digital government services. This objective is further reinforced by establishing and activating a business continuity management system, verifying its effectiveness, and pursuing continuous improvement.

In this version, DGA updated the controls related to the activation phase of the Business Continuity Management System, particularly those addressing the development of disaster recovery plans for information and communication technology. These updates enhance the readiness of government agency by providing and testing technical alternatives and solutions. Furthermore, the classification matrix for platforms, applications, and services was updated to serve as a comprehensive framework. Collectively, these efforts aim to ensure the reliability and continuity of digital government services across government agency.

3. Objectives

These controls aim to enable government agency to ensure the sustainability of digital government services and core operations, while mitigating potential risks, through the following:

1. Identify appropriate treatment strategies and plans for addressing incidents and crises.

2. Proactively identify risks to ensure business continuity, digital services, and the agency's core operations.

3. Support decision-making and optimize the allocation of resources, capabilities, and supply chain continuity.

4. Raise awareness about risk management and business continuity to prepare for, respond to, and recover from incidents.

5. Enhance the integration among government agency and strengthen national resilience and flexibility.

4. Scope

DGA developed these controls to establish the requirements for risk management and business continuity in digital government, as outlined below:

Risk Management Controls: To enhance the readiness of digital government agency and strengthen their ability to respond to risks, Figure 1 illustrates the implementation process of these controls. This includes establishing and governing a risk management system, assessing and addressing risks through the activation of risk management processes, as well as training and continuous improvement in risk management.

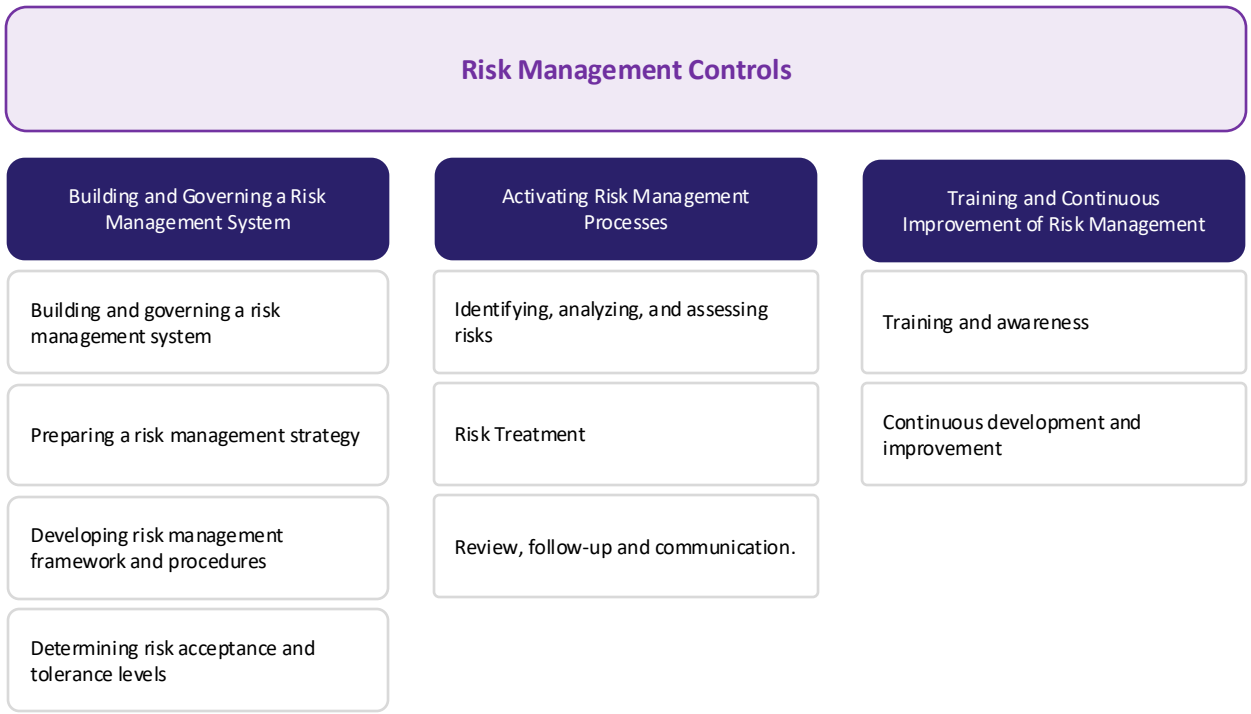

Figure 1: Risk Management Controls

Business Continuity Controls: To contribute and assist in planning to build an integrated business continuity system, through which its system is activated, and then the system is verified and corrected, which achieves high effectiveness in managing and improving business continuity in the government agency. Figure 2 illustrates the mechanism for applying these controls.

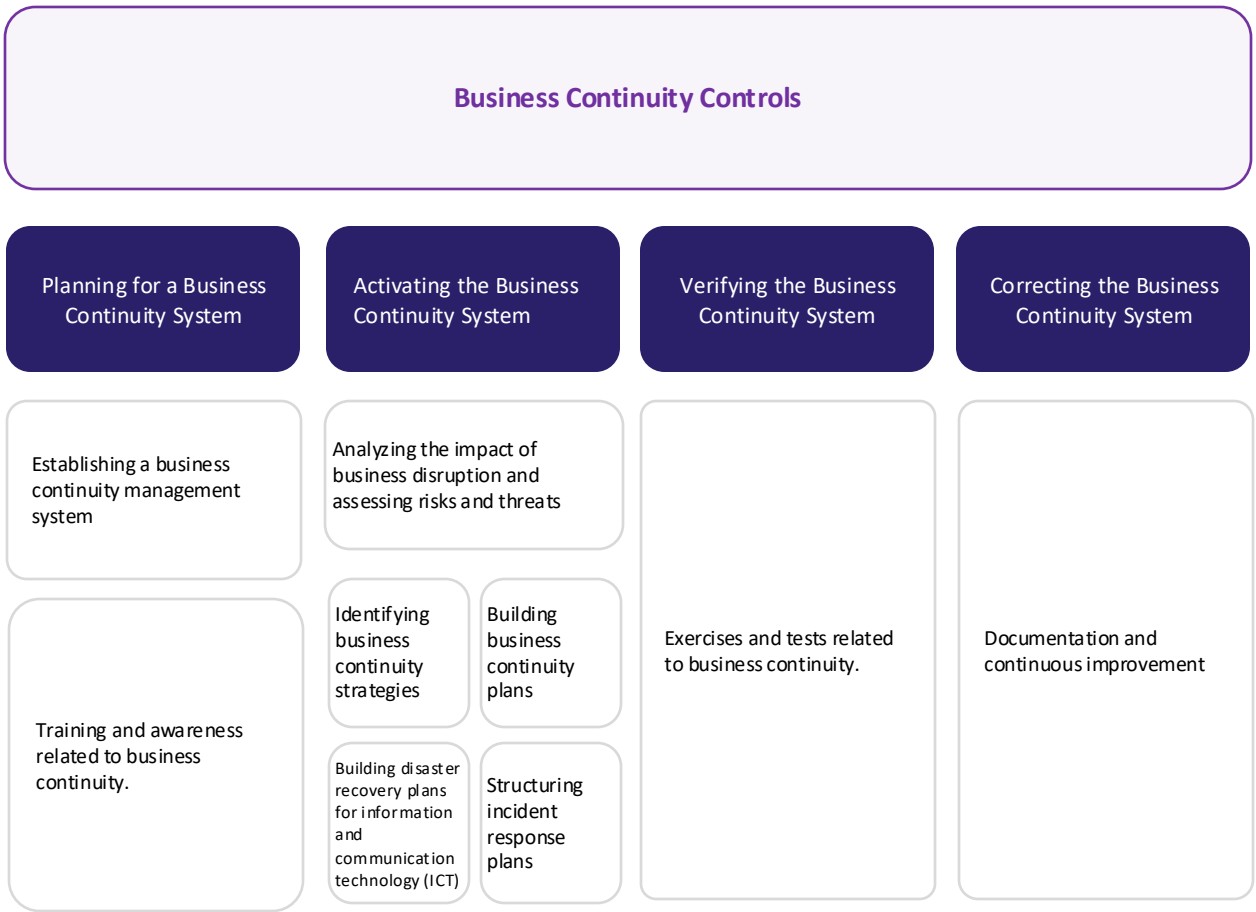

Figure 2: Business Continuity Management Controls

5. Applicability

The requirements and standards set forth herein shall apply to all government agency providing digital services and products, as well as to operators, regardless of their type, size, or nature. Their applicability shall be determined based on the agency's operating environment, level of complexity, and number of geographical locations.

6. Implementation and Compliance

Refined: Pursuant to paragraph 9 of Article 4 of the Digital Government Authority Regulation—which stipulates that the Authority shall **"develop the technical standards for digital transformation models in government sectors and follow up on compliance with them, in coordination with the relevant authorities"**, DGA shall assess and measure the extent to which government agency comply with these controls following the mechanism determined by the DGA.

7. Risk Management Controls

7.1 Building and Governing a Risk Management System

7.1.1 Building and Governing a Risk Management System		
Objective	Establishing the components and elements of risk management system governance, and defining the roles, responsibilities, and authorities of stakeholders, to support the effective implementation of the ri sk management system within the agency and ensure its alignment with the agency's strategic objecti ves.	
Government agency should comply with the following:		
Control number:		
05-107-01	Establish an administrative unit responsible for the risk management system within the agency, in proportion to the agency's approved organizational structure, with the implementation of the following minimum requirements:	
	5-107-01.01	Appoint a qualified individual with the necessary qualifications and authority as the manager of the risk management system.
	5-107-01.02	Define the roles and responsibilities within the risk management system.
	5-107-01.03	Appoint a team to carry out the roles, responsibilities, and tasks within the risk management system based on the needs and activities of the agency.
05-107-02	The senior management of the government agency shall establish a steering committee to oversee the work of the risk management system in the agency from the senior management, headed by the first official in the agency or his/her deputy.	
05-107-03	Develop the charter of the steering committee responsible for the risk management system after its approval and dissemination by the senior management of the agency, to include the following as a minimum	
	5-107-03.01	Scope and objectives of the committee.
	5-107-03.02	Identify a chairman, members, and secretary for the committee that has been formed.
	5-107-03-03	Roles, responsibilities, and authorities of the chairman, members, and secretary of the committee.
	5-107-03.04	Regularity of meetings (quarterly at a minimum), and a mechanism for documenting meetings and following up on decisions
	5-107-03.05	Approval by the authorized person as the agency deems appropriate.
05-107-04	Establish and approve a risk management policy in line with the agency's objectives and share it with stakeholders, to include the following as a minimum:	
	5-107-04.01	Introduction and definition of risk management policy.
	5-107-04.02	Objectives of establishing a risk management policy.
	5-107-04.03	Scope of application of risk management with clarification of the relationship with external parties, suppliers, and exceptions.
	5-107-04.04	The organizational and administrative structure of the risk management system.
	5-107-04.05	General controls for risk management policy.
	5-107-04.06	Roles, responsibilities, and authority matrix for internal and external stakeholders.
	5-107-04.07	Mechanism for periodic review of risk management policy.
	5-107-04.08	Approval by the authorized person as the agency deems appropriate.

7.1.2 Activating Risk Management Processes		
Objective	Developing a risk management strategy to define the strategic direction of risk management in the agency and developing a roadmap to achieve the targeted maturity level in risk management.	
Government agency should comply with the following:		
Control number:		
05-107-05	Assess the current maturity level of the risk management system in the agency and determine the targeted maturity level to be reached within a specific time frame.	
05-107-06	Develop and approve a risk management strategy and share it with the agency's stakeholders. At a minimum, the strategy shall include the following:	
	5-107-06.01	Risk management vision and mission.
	5-107-06.02	Risk management objectives.
	5-107-06.03	Aligning risk management strategy with Vision 2030, the agency's strategy and objectives.
	5-107-06.04	A roadmap for implementing the targeted maturity level in the risk management system.
	5-107-06.05	The initiatives and resources needed to reach the targeted maturity level.
	5-107-06.06	Indicators for measuring the implementation of the strategy initiatives across the entire agency.
	5-107-06.07	Mechanism for periodic review of risk management strategy.
	5-107-06.08	Approval by the authorized person as the agency deems appropriate.
05-107-07	Implement the roadmap to achieve the strategic objectives of risk management and reach the targeted maturity level.	

7.1.3 Developing risk management framework and procedures		
Objective	Establishing a framework for risk management governance involves identifying, assessing, and analyzing internal and external risks, as well as determining possible strategies to mitigate their impact and/or likelihood of occurrence.	
Government agency should comply with the following:		
Control number:		
05-107-08	Develop and approve a risk management framework document and share it with stakeholders to include the following as a minimum:	
	5-107-08.01	Determining the context, scope, and objectives of the risk management framework and linking them with the agency's objectives.
	5-107-08.02	Determining the risk management methodology in the agency and aligning it with the services and products provided to stakeholders, considering the regulations issued by the relevant agency.
	5-107-08.03	Identifying the main risk categories in the agency.
	5-107-08.04	Determining the probability levels, impact, and risk assessment matrix.
	5-107-08.05	Identifying the types of controls and the mechanism for evaluating their effectiveness.
	5-107-08.06	Determining the methodology for selecting risk treatment strategies and how to deal with them.
	5-107-08.07	Determining the mechanism for analyzing and evaluating the inherent and residual risks in the agency.
	5-107-08.08	Determining the mechanism for implementing treatment plans, including the maximum implementation deadlines and risk assessment results.
	5-107-08.09	Determining a mechanism and criteria to identify the most important or major risks in the agency.
	5-107-08.10	Determining the mechanism for Key Risk Indicators (KRIs).
	5-107-08.11	Determining the mechanism for reviewing and monitoring risks of all types and levels in the agency.
	5-107-08.12	Determining the mechanism for communication and consultation regarding risks in the agency, whether internally or externally.
	5-107-08.13	Determining the mechanism for reporting risks to stakeholders and relevant committees inside and outside the agency.
	5-107-08.14	Determining risk escalation mechanisms.
	5-107-08.15	Determining the mechanism for reviewing the risk management framework document.
	5-107-08.16	Approval by the authorized person as the agency deems appropriate.
05-107-09	Develop a risk champions document in the agency to coordinate, implement, and follow up on risk management activities and submit related reports to include the following as a minimum:	
	5-107-09.01	Criteria for identifying risk champions and the required competencies and skills.
	5-107-09.02	Roles and responsibilities of risk champions.

05-107-10	Build a risk reporting system for all members of the agency, to include the following as a minimum	
	5-107-10.01	Risk reporting document.
	5-107-10.02	Reporting mechanism includes templates and a unified channel for reporting risks.
05-107-11	Develop and approve risk management procedures and share them with stakeholders to ensure the following as a minimum:	
	5-107-11.01	Determining the risk context.
	5-107-11.02	Identifying and analyzing internal and external threats.
	5-107-11.03	Assessing internal and external risks and threats.
	5-107-11.04	Treating internal and external risks and threats.
	5-107-11.05	Monitoring, reviewing, and following up on internal and external threats.
	5-107-11.06	Communication and consultation.
	5-107-11.07	Approval by the authorized person as the agency deems appropriate.
05-107-12	Develop a risk register template for all administrative units within the agency and update it periodically to include, at a minimum, the following:	
	5-107-12.01	Risk identifier.
	5-107-12.02	Risk owner.
	5-107-12.03	Risk description.
	5-107-12.04	Risk root causes and consequences.
	5-107-12.05	Assessment of inherent risk (inherent impact, inherent probability, and inherent severity).
	5-107-12.06	Controls are implemented to reduce the impact and probability of the risk.
	5-107-12.07	Evaluation of the effectiveness of the implemented controls.
	5-107-12.08	Assessment of residual risk (inherent severity and effectiveness of implemented controls).
	5-107-12.09	Risk treatment strategy.
	5-107-12.10	Treatment plans to be implemented to deal with the risk.
	5-107-12.11	Risk treatment plan owner.
	5-107-12.12	Risk treatment plan completion date.
	5-107-12.13	Percentage and status of implementation of risk treatment plans.
05-107-13	Develop a dashboard to display risk statistics for the agency, including but not limited to risk number, classifications, assessment, etc.	
05-107-14	Develop an annual plan to assess the risks of all administrative units in the agency and approve it by the authorized person as the agency deems appropriate.	

7.1.4 Determining Risk Acceptance and Tolerance Levels		
Objective	Establish and define the agency's risk appetite and tolerance levels, based on its strategic directions a nd senior management directives, to enable the prioritization of risk treatment.	
Government agencies should comply with the following:		
Control number:		
05-107-15	Develop and approve a document on the agency's risk acceptance and tolerance levels, in line with its strategic directions and objectives, and share it with stakeholders. At a minimum, the document shall include the following:	
	5-107-15.01	Defining risk acceptance and tolerance levels.
	5-107-15.02	Determining the methodology for risk acceptance and tolerance levels.
	5-107-15.03	Specifying the roles and responsibilities for the processes of determining and approving risk acceptance and tolerance levels.
	5-107-15.04	Defining risk acceptance and tolerance levels and limits.
	5-107-15.05	Determining the mechanism for monitoring and reporting risk acceptance and tolerance levels to stakeholders and relevant parties.
	5-107-15.06	Establishing a mechanism for reviewing the risk acceptance and tolerance levels document.
	5-107-15.07	Approval by the authorized person as the agency deems appropriate.

7.2Activating Risk Management Processes

7.2.1 Identifying, Analyzing, and Assessing Risks		
Objective	Identifying and assessing internal and external risks, determining their likelihood of occurrence, and e valuating their potential impact on the achievement of objectives and strategies.	
Government agency must commit to the following:		
Control number:		
05-107-16	Identify, analyze, and assess the most important or major risks at the agency level using a top-down or bottom-up approach.	
05-107-17	Identify KRIs at the agency level.	
05-107-18	Understand the working environment to identify internal and external risks and threats at the agency and administrative unit levels, as a minimum:	
	5-107-18.01	Understanding the operational processes of the administrative units.
	5-107-18.02	Conducting brainstorming sessions with risk owners and champions.
	5-107-18.03	Reviewing previous internal and external audit reports.
05-107-19	Identify and reflect internal and external risks and threats in the agency's risk register, to include, as a minimum: • A description of the risk, including the name of the risk, its main causes, and the consequences of its occurrence. • The root causes and consequences of risks and threats. • Linking risks and threats to the agency's strategic and operational objectives. • Identifying the risk owner. • Documenting the date the risk was identified. • Determining the classification of the main risk categories. • Monitoring and documenting all information in the risk register.	
05-107-20	Analyze and assess internal and external risks and threats and reflect them in the agency's risk register, to include as a minimum:: • Determining the inherent severity by determining the level and degree of probability and impact. • Identifying the controls implemented to reduce the impact and probability of the risk. • Evaluation of the effectiveness of the implemented controls. • Determining the residual severity. • Monitoring and documenting all information in the risk register	

7.2.2 Risk Treatment		
Objective	Developing appropriate solutions to address risks in order to reduce their likelihood of occurrence and/ or mitigate their consequences.	
Government agency must commit to the following:		
Control number:		
05-107-21	Identify appropriate treatment plans for the most important or major risks at the agency level and their completion dates.	
05-107-22	Identify and reflect appropriate treatment plans for each risk in the agency's risk register, to include as a minimum:	
	5-107-22.01	The risk treatment strategy adopted according to the risk management framework after studying the required costs, resources, and benefits.
	5-107-22.02	The approved treatment plans to be implemented to deal with the risk.
	5-107-22.03	Risk treatment plan owner.
	5-107-22.04	Risk treatment plan completion date.
	5-107-22.05	Status and percentage of implementation of the risk treatment plans.
	5-107-22.06	Monitoring and documenting all information in the risk register.
05-107-23	Share and approve the risk register of the relevant administrative unit by the risk owners and the first responsible person of the administrative unit.	
05-107-24	Submit periodic reports on the results of the risk assessment to the steering committee responsible for the risk management system, as well as to stakeholders and interested parties, in accordance with the reporting frequency established in the risk management framework.	

7.2.3 Review, Follow-up and Communication		
Objective	Monitoring and following up on risks to ensure the quality and effectiveness of the risk assessment and treatment processes.	
Government agency must commit to the following:		
Control number:		
05-107-25	Update the agency's risk register by the risk management officials, by applying as a minimum:	
	5-107-25.01	Periodically monitor and follow up on the status of the agency's identified internal and external risks.
	5-107-25.02	Periodically monitor controls and evaluate their effectiveness.
	5-107-25.03	Periodically monitor the effectiveness of treatment plans.
	5-107-25.04	Periodically monitor the implementation rates of risk treatment plans within the specified period of time.
05-107-26	Updating the most important or major risks and KRIs on a regular basis.	
05-107-27	Submit risk reports to senior management, internal and external committees, stakeholders, and interested parties based on the periodicity adopted in the risk management framework, including but not limited to: • Comprehensive risk status report. • Top risks report. • KRIs report.	

7.3Training and Improvement of the Risk Management System

7.3.1 Training and Awareness	
Objective	Training all employees and stakeholders, and raising awareness of risk management, to ensure the ac hievement of the agency's objectives and strategies.
Government agency must commit to the following:	
Control number:	
05-107-28	Analyze training needs in cooperation with the agency's human resources unit to understand the training requirements for risk management.
05-107-29	Develop and implement a training plan for risk management staff and risk champions consistent with the roles and responsibilities in the agency's risk management system.
05-107-30	Develop and implement a plan for risk management awareness campaigns for agency staff to promote a risk culture using one of the following activities: • Awareness messages through various communication channels. • Global and local news reports and publications related to risks. • Awareness workshops, meetings, and open discussions. • Risk awareness week. • Digital learning platforms.
05-107-31	Review and update the awareness campaign plan and disseminate risk management culture in the agency annually.

7.3.2 Continuous Development and Improvement		
Objective	Reviewing risk management procedures and processes to improve the agency's capacity, enhance the effectiveness of the risk management system, and apply best practices and standards.	
Government agency must commit to the following:		
Control number:		
05-107-32	Review and update the risk management system documentation regularly according to the approved review mechanism for each document or when there is a fundamental change in the agency's strategic or operational objectives, as a minimum:	
	5-107-32.01	Risk Management Policy.
	5-107-32.02	Risk Management Strategy.
	5-107-32.03	Risk Management Framework.
	5-107-32.04	Risk Management Procedures.
	5-107-32.05	Risk Tolerance and Acceptance Levels Document.
05-107-33	Use and develop standardized templates to implement risk management processes at the agency level, including but not limited to (Risk Register, Risk Escalation and Acceptance Forms, Risk Reports, Risk Dashboards).	
05-107-34	Develop a mechanism for storing and archiving risk management system data and documents to ensure the continuity of the administrative unit's operations.	
05-107-35	Review the effectiveness of the implementation and application of the risk management system annually using one of the following review methods: • Self-assessment. • Key Performance Indicator (KPI) Assessment. • Internal or external audit/review.	
05-107-36	Implement and develop an annual plan to assess compliance with relevant regulatory controls.	
05-107-37	Submit reports on the results of the review of the effectiveness of the implementation and application of the risk management system, as well as the results of the compliance assessment to senior management and the steering committee responsible for the risk management system, ensuring that appropriate corrective actions are taken.	

8. Business Continuity Controls

8 .1Planning for a Business Continuity System

8.1.1 Establishing a Business Continuity System		
Objective	Developing the general framework and defining the roles and responsibilities of stakeholders and rele vant departments in planning, implementing, reviewing, and enhancing the business continuity system .	
Government agency must commit to the following:		
Control number:		
05-107-38	Appoint a Business Continuity Manager with the qualifications and authority to oversee the business continuity system.	
05-107-39	Appoint a team to carry out the roles and responsibilities in the business continuity system, consisting of a sufficient number of qualified employees.	
05-107-40	Establish a steering committee responsible for monitoring the implementation of the business continuity system in the agency.	
	5-107-40.01	The steering committee for the business continuity system shall be chaired by the head of the agency or his/her deputy, and its membership shall include, at a minimum, the following: the business continuity officer, information technology officer, cybersecurity officer, facilities, security and safety officer, risk management officer, human resources officer, communication and media officer, and finance and procurement officer, in addition to any other concerned parties.
	5-107-40.02	The committee shall have the necessary powers to support the business continuity system, and its scope of authority, powers, and membership must be clarified.
05-107-41	Develop a Business Continuity Policy, to include the following as a minimum:	
	5-107-41.01	Documentation, approval, and dissemination of the policy within the agency.
	5-107-41.02	Aligning the policy with the agency's vision, mission, and values.
	5-107-41.03	Determining the scope of application of the business continuity system, specifying any exceptions to the application, if any.
	5-107-41.04	Defining the business continuity system and its components in the agency.
	5-107-41.05	Including key suppliers of priority products and services within the scope of the business continuity system.
	5-107-41.06	Including an internal distribution list for stakeholders.
	5-107-41.07	Reviewing the policy periodically following the agency's policy review system or when there is a fundamental change in the operating environment or strategic objectives of the agency.

05-107-42	Develop a business continuity framework for the agency, which shall include, as a minimum:	
	5-107-42.01	Business continuity system strategy.
	5-107-42.02	Identifying internal operations and external operating factors as part of the strategic direction for business continuity in the agency.
	5-107-42.03	Business disruption impact analysis.
	5-107-42.04	Risk and threat assessment.
	5-107-42.05	Strategies for business continuity plans and technical and communication disaster recovery plans.
	5-107-42.06	Structuring incident response plans.
	5-107-42.07	Exercises and tests.
	5-107-42.08	Training and awareness.
	5-107-42.09	Documentation and continuous Improvement.
05-107-43	Strengthening the business continuity system by assigning responsibilities to the following roles as a minimum:	
	5-107-43.01	Business continuity plan owners from the relevant departments.
	5-107-43.02	Business continuity plan coordinators from the relevant departments (business continuity champions).
	5-107-43.03	Technical and communications disaster recovery teams for the business continuity system.
05-107-44	Submit regular business continuity reports to senior management or the Business continuity Steering Committee, chaired by the Head of the agency or their delegate.	

8.1.2 Training and awareness of the business continuity system		
Objective	Raise awareness among all employees and relevant parties about business continuity and strengthen their training on roles and responsibilities within the scope of the business continuity system.	
Government agency must commit to the following:		
Control number:		
05-107-45	Conduct a training needs analysis, in collaboration with Human Resources, to define training requirements tailored to the skills necessary for the business continuity system.	
05-107-46	Ensure the integration of employee training on multiple skills to manage the business continuity system and develop succession plans (to avoid single points of failure) for business continuity activities.	
05-107-47	Implement a program to disseminate a business continuity culture within the agency through training and specialized workshops for all parties participating in the business continuity system at least once a year and when a fundamental change occurs in the agency's operational processes.	
	5-107-47.01	Prepare and implement awareness campaigns for the business continuity system through the following channels, for example: • Awareness Messages • Newsletters • Awareness Banners • The agency's internal website (internal digital portal) • Open discussion meetings and sessions • Workshops
05-107-48	All employees of the agency should be aware of the policy, their roles and responsibilities, and the impact of not implementing and supporting the business continuity system.	

8.2 Activating the Business Continuity System

8.2.1 Analyze the impact of business disruption and assess risks and threats		
Objective	Analyze the impact of operational disruptions on the delivery of products and services; identify and ass ess internal and external risks, threats, and critical failure points that could affect them; and determine the target recovery time for essential services after a disruption.	
Government agency must commit to the following:		
Control number:		
05-107-49	Include all internal and external operations and procedures carried out by the agency and determine the internal and external accreditations.	
05-107-50	Appoint owners for the processes and procedures that are included.	
05-107-51	Analyze the impact of business interruptions using a business impact analysis matrix adopted by the agency, based on the level of impact acceptance and the risks specific to the agency.	
	5-107-51.01	At a minimum, the business impact analysis matrix should include the following categories: • Operational Impact. • Financial Impact. • Legal, Regulatory, and Strategic Impacts. • Reputation impact
05-107-52	Continuously assess and review risks and threats to the continuity of the agency's operations, aligning them with the risk management methodology adopted by the agency.	
05-107-53	Identify and monitor risks and threats that may lead to interruptions or disturbances in the priority operations and procedures of the agency, aligning them with relevant stakeholders.	
05-107-54	Determine the effects of internal and external risks on the agency's operations and procedures.	
05-107-55	Identify and evaluate the controls applied to deal with risks and threats that affect the continuity of the agency's business.	
05-107-56	Identify additional or compensatory controls appropriate to address the risks and threats affecting the continuity of the agency's operations.	
05-107-57	Determine the Maximum Tolerable Period of Disruption (MTPD) for the disruption of products, services, operations, and activities.	
05-107-58	Taking into account the Minimum Business Continuity Objectives (MBCO) or the minimum level of service delivery.	
05-107-59	Determine the target period for restoring critical business services, Recovery Time Target (RTO).	
05-107-60	Classify the level of importance of government services, platforms and applications and adhering to the targeted recovery times for each level according to Platforms, Applications and Service Classification Matrix issued by the Digital Government Authority (DGA) via Raqmi Portal.	
05-107-61	Determine the human, logistical, technical, infrastructure, and alternative procedures necessary to implement the service or procedure after the interruption.	
05-107-62	The individual in charge of managing the business continuity system is required to submit a comprehensive report on the business impact analysis to the Steering Committee for approval.	
05-107-63	Present the results of the risk and threat assessment to the Business Continuity Steering Committee as part of the results of the Business Disruption Impact Analysis for approval.	
05-107-64	Review the Business Disruption Impact Analysis at least annually, or when a significant change occurs in the agency's operational processes or strategic objectives.	

8.2.2 Determine Business Continuity Recovery Strategies		
Objective	Ensure the integration of employee training across multiple skills for managing the business continuity system, and develop succession plans to avoid single points of failure in business continuity activities.	
Government agency should comply with the following:		
Control number:		
05-107-65	Define business continuity recovery strategies based on the results of the business impact analysis and risk and threat assessments. At a minimum, these strategies shall include:	
	5-107-65.01	Communication Systems and Information Technology.
	5-107-65.02	External Technical Servers and Cloud Technologies Used.
	5-107-65.03	Remote Work Solutions and Alternative Workplace Solutions.
	5-107-65.04	Backup Storage Mechanisms and Backup Systems.
05-107-66	Cost-benefit analysis to measure the effectiveness of business continuity strategies and solutions, prioritize them, and adopt them by the Business Continuity Steering Committee.	
05-107-67	Identify key suppliers and outsourced services according to the outputs of the business disruption impact analysis. Both suppliers and services must undergo further scrutiny to ensure the resilience of supply chains. Supplier testing and management requirements include:	
	5-107-67.01	Classification of performance according to service level agreements.
	5-107-67.02	Determine the target recovery time and target recovery point in concluded contracts.
05-107-68	Review recovery strategies at least annually, or when a significant change occurs in the operational or strategic objectives of the agency.	

8.2.3 Developing Business Continuity Plans		
Objective	Develop and document actions derived from the outcomes of the selected strategies and solutions.	
Government agency should comply with the following:		
Control number:		
05-107-69	Prepare business continuity plans based on approved business continuity strategies, ensuring they include at least:	
	05-107-69.01	Plan Scope.
	05-107-69.02	Executive Summary and Purpose.
	05-107-69.03	Owner's Name of the Plan and Document Properties.
	05-107-69.04	Individuals and Teams Responsible for Incident Response.
	05-107-69.05	Roles and Responsibilities of Involved Teams Before, During, and After Disruptions.
	05-107-69.06	Required Resources for Implementing Priority Operations and Procedures.
	05-107-69.07	The procedures for recovering operations and priority procedures, including alternatives and actions to be taken in the event of a complete digital service outage, along with an explanation of the internal and external dependencies in the implementation mechanism.
	05-107-69.08	Activation and Deactivation Mechanism of the Plan and Escalation Matrix.
	05-107-69.09	Communication Data for the Main Team, Supporting Teams, and External Suppliers for Plan Execution.
05-107-70	Review and test plans at least once a year or whenever a fundamental change occurs within the agency.	

8.2.4 Develop Disaster Recovery Plans for Information and Communication Technology (ICT)		
Objective	Develop and document the agency's IT capabilities to restore critical systems to an acceptable level of service within a predefined period following a disruption. The Disaster Recovery Plan for Information T echnology is designed to ensure the agency's ability to respond to crises, disruptions, or emergencies affecting its information systems and digital services, thereby minimizing the impact on its operations.	
Government agency should comply with the following:		
Control number:		
05-107-71	Providing backup data centers for critical and sensitive platforms and applications within the agency, according to the results of the business impact analysis.	
05-107-72	Providing backup and alternative communication circuits for the communication lines that serve the agency's critical sensitive systems and services from different service providers, using various technologies.	
05-107-73	Conducting regular tests for backup and alternative communication circuits to ensure their effectiveness and the continuity of digital services.	
05-107-74	Creating Information and Communication Technology (ICT) recovery plans involves restoring platforms, applications, digital services, and data promptly to achieve the targeted recovery time for the agency. It must include, as a minimum:	
	5-107-74.01	Roles and responsibilities for activating and terminating Disaster Recovery Plans for Information and Communication Technology (ICT)
	5-107-74.02	Procedures and responsibilities for recovering Information and Communication Technology (ICT) systems and assets at primary and alternate sites according to priority.
	5-107-74.03	Internal notification procedures in the IT department/ unit, including procedures for notifying users during routine operations.
	5-107-74.04	Mechanism for sharing stakeholders with a copy of the agency's structure along with the information and communication tree of the participating teams, and supplier data for technology and communication services.
	5-107-74.05	How to determine the causes of disruption, assess the probability of further disruptions, evaluate the status of physical infrastructure and functionalities of IT equipment, and access inventory
	5-107-74.06	The timeline for prioritizing operation and procedure recovery is based on their importance and recovery time objective.
	5-107-74.07	Escalation matrices, including the teams and individuals responsible for each escalation or awareness action. Taking into account the critical business monitoring system that operates 24/7.
	5-107-74.08	Procedures for returning to normal operations.
	5-107-74.09	Procedures for verifying the recovered data and its accuracy.
	5-107-74.10	System functionality testing procedures and verification checks to ensure that the system is operating correctly.
	5-107-74.11	Procedures for cleaning systems, including evidence sites, documents, and related backup media.
	5-107-74.12	Procedures for announcing the completion of recovery efforts and testing, and the return of systems to normal operation, after approval from the owners of the communication and information technology systems, and information assets.

05-107-75	Determine backup and recovery methods and strategies to quickly and effectively restore system operations after a service disruption. It must include, as a minimum:	
	5-107-75.01	Strategies for various changes such as mobile device sites, backup locations, and cloud services for disaster recovery as a service.
	5-107-75.02	Procedures to ensure full system backup according to recovery procedures.
05-107-76	Communicate with the Digital Government Authority in the event of disruption to digital services, according to the “Guide for a User to Report an Interruption in Digital Government Services” on Raqmi Portal.	
05-107-77	Providing the availability percentages of the platforms and applications affiliated with the agency to the Digital Government Authority on a monthly basis, along with supporting evidence to validate the submitted percentages through "the service for updating the availability rates of digital government services“ on Raqmi Portal.	
05-107-78	Document incidents in the case of a disruption to operations, explaining responsibilities and authorities related to collecting, approving, and updating activity logs, function test results and data, lessons learned, and post-incident reporting.	
05-107-79	Approval of Disaster Recovery Plans for Information and Communication Technology (ICT) is the responsibility of the Chief Information and Communications Technology Officer (CIO), following their review with relevant stakeholders.	
05-107-80	Ensuring the activation of information security controls and cybersecurity measures at all times, especially when activating the Disaster Recovery Plans for Information and Communication Technology (ICT) for backup sites.	
05-107-81	Testing the Information and Communication Technology disaster recovery plans, including the activation of backup data centers and the restoration of critical and sensitive platforms and applications within the agency at least once a year, or whenever there is a significant change to the agency's IT infrastructure.	

8.2.5 Structuring Incident Response Plans		
Objective	Define the structure of incident response plans and the mechanism for activating business continuity p lans, together with an internal and external communication plan to be followed during incidents.	
Government agency should comply with the following:		
Control number:		
05-107-82	Create an incident response plan, which should include, at a minimum:	
	5-107-82.01	Identify incident response teams or individuals and their connection with emergency response teams and crisis management teams.
	5-107-82.02	Include procedures for identifying damage assessment teams or individuals and specify the reporting and escalation mechanism.
	5-107-82.03	Include the necessary resources for incident response, such as personnel and communication methods during incidents, supplies and resources, among others.
	5-107-82.04	Determine the mechanism for activating and deactivating the plan.
	5-107-82.05	Determine an escalation mechanism for incidents internally and externally.
	5-107-82.06	Identify the call tree for the response team and designate representatives for each member, update communication information, and test it periodically.
05-107-83	Create and approve a media communication and response plan.	
05-107-84	Document procedures for dealing with relevant external parties (before, during, and after).	
05-107-85	Regularly review and test the incident response plan, ensuring it is done at least once a year or whenever there is a significant change in the operational or strategic objectives of the agency.	

8.3 Verify the Business Continuity System

8.3.1 Exercises and Tests Related to Business Continuity		
Objective	Measure the effectiveness of the business continuity plans and the incident response structure to ensure the proper implementation of the business continuity policy and the achievement of business continuity objectives.	
Government agency must commit to the following:		
Control number:		
05-107-86	Create a schedule for all tests and exercises for various business continuity plans and adopt them annually by the Business Continuity Steering Committee. It should include different scenarios, such as: • Current risks and threats • Risks identified as arising from future technologies. • Actual incidents such as cyber-attacks, headquarters fires, pandemics, supply chain outages, etc.	
05-107-87	Implement the testing and exercises program approved by the Business Continuity Steering Committee.	
05-107-88	Create testing and exercise reports, which should include, at a minimum:	
	5-107-88.01	Executive Summary.
	5-107-88.02	Plan and its Execution Date.
	5-107-88.03	Exercise or Test Results, and the Next Execution Date.
	5-107-88.04	Exercise or Test Scenario.
	5-107-88.05	Teams Participating in the Exercise or Test.
	5-107-88.06	Exercise or Test Phases.
	5-107-88.07	The achieved timeframes compared to the targeted times (Targeted Recovery Time/ Recovery Point Objective).
	5-107-88.08	Corrective actions or recommendations with dates and responsibilities for execution.
05-107-89	Share testing and exercises with Business Continuity Steering Committee members.	

8.4 Correct the Business Continuity System

8.4.1 Documentation and Continuous Improvement		
Objective	Document lessons learned from implementing the business continuity system, including real incidents, exercises, tests, and review results. Conduct routine maintenance activities to sustain and improve the system after its establishment. This process shall enhance organizational resilience and strengthen th e management system's effectiveness through periodic reviews, effective resolution of non-conformitie s, and the implementation of corrective actions.	
Government agency must commit to the following:		
Control number:		
05-107-90	Review the business continuity system periodically (at least annually) through an internal or external auditor with sufficient qualifications and experience.	
05-107-91	Ensure the development and regular updating of business continuity plans, technical and communications disaster recovery plans, the media response plan, and the incident response plan, based on the outputs of the verification phase. These plans shall also take into account at least the following minimum factors:	
	5-107-91.01	Post-Incidents Reports.
	5-107-91.02	Results of Audits.
05-107-92	Share the results of internal and external audits with concerned parties to ensure corrective actions are taken.	

9. Table of Definitions

Unless the context requires otherwise, the following words and phrases, wherever they appear in this document, are intended to have the meanings specified next to each of them.

Term	Definition
DGA	Digital Government Authority
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 agency	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.
Risks	The probability of an event occurring that will have negative or positive effects.
Internal and External Risks	Internal or external incidents that may affect the achievement of the agency's strategic objectives.
Risk Management	Apply strategies, policies, and procedures to prevent the emergence of new risks, reduce existing ones, and manage residual risks. This includes anticipating, identifying, analyzing, evaluating, prioritizing, monitoring, and reviewing risks, as well as preventing and mitigating their negative effects.
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.

Term	Definition
Roles and Responsibility Matrix	A documented framework that illustrates the allocation of roles and responsibilities assigned for performing tasks.
Risk Management Strategy	The approach followed by the agency to manage risks and reach the most appropriate solutions to reduce the impact of risks on the agency.
Risk Acceptance Level	The level and type of risks that the organization 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 for identifying, analyzing, and evaluating risks, treating them, and following them up periodically at the agency.
Risk Evaluation	A quantitative or qualitative approach to identifying and analyzing potential risk events and calculating their likelihood and impact, considering factors of exposure and vulnerabilities.
Risk Owner	The party responsible for managing a specific risk within its jurisdiction and mandate. Its responsibilities include anticipating, identifying, analyzing, assessing, prioritizing, monitoring, reviewing, preventing, mitigating, preparing for, responding to, and recovering from that risk, in coordination with supporting and assisting the agency.
Owner of Risk Treatment Plans	The individual or party authorized to implement and execute risk response plans and report their status to risk management and stakeholders.
Risk Champions	Those nominated by the authorities to represent the risk management within the various main departments of the agency, to coordinate, monitor, and execute risk management tasks and submit related reports.
Impact	The resulting consequences in case a risk occurs.
Likelihood	The extent to which a risk can occur and recur within a specific period.
Inherent Risks	Preliminary risks before implementing any mitigation measures to reduce the impacts resulting from them.
Residual Risk	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	A measure used to monitor changes in the level of risk exposure and is used as an early warning sign for risks.

Term	Definition
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 Management	Applying the necessary strategies, policies, and procedures to ensure the continuity of providing core services and products during emergencies, crises, and disasters. And developing strategies, solutions, and plans to ensure the continuation of the work.
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.
Business Continuity Policy	An approved document that defines the agency's business continuity governance, its scope, objectives, and responsibilities, as well as the authorities related to implementing business continuity management.
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 Impact Analysis	Analysis of business processes and activities related to providing core services products, and the effects of disruption of those processes.
Risk Register	A document that contains a comprehensive list of risks, along with detailed information for each risk. This includes, at a minimum: risk registration date, risk code, risk title, sector, risk owner, risk classification, risk description, risk occurrence scenario, likelihood level, impact level, risk level, confidence level in probability and impact assessments, affected areas, key risk indicators, mitigation strategies, preventive measures, key control indicators, response and recovery plans, agency involved in response, agency involved in recovery, and support and backup agency.
Compliance and Conformity	The agency fulfills the necessary requirements in the required manner.
Continuous Improvement	An ongoing activity to enhance the performance of the risk management and business continuity system.
Top Management	All individuals who are responsible for making key decisions within the agency.
Corrective Action	Steps or measures that mitigate the severity of the effects resulting from incidents.
Data validation testing	Process enables the user to verify the compatibility of the retrieved data they are using with the provided working conditions.
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.
Exercises	An activity in which business continuity plans are fully or partially trained to ensure they contain the appropriate information and achieve the desired results when activated.

10. Table of Abbreviations

Abbreviation	Description
KRIs	Key Risk Indicators
MTPD	Maximum Tolerable Period of Disruption
MBCO	Minimum Business Continuity Objective
RTO	Recovery Time Objective

11. Appendices

11 .1Platforms, Applications and Services Classification Matrix

Classification Level*	Stakeholder Impact in Case of Disruption	Financial impact in Case of Disruption	Legal and Regulatory Impact in Case of Disruption	Reputational Impact in Case of Disruption	Recovery Time Objective RTO**
Very Critical	A comprehensive impact on the digital platforms and applications provided throughout the Kingdom to include all the following stakeholders: • government agency • Business and Supply Chains • Citizens and Residents Or the service is provided to senior officials or key figures in the Kingdom. Or the service is associated with a peak season or a specific time period for utilization.	Financial losses amounting to 1,000,000 Saudi Riyals per hour. 0.0115% of the total annual financial return from this service (whichever is greater).	Results in the loss of compliance certification (local/international) or exposure to litigation and penalties by local authorities or international courts for violating local or international laws.	Results in damage and a negative impact on the reputation of the digital government in local and/or international media, leading to a decline in Saudi Arabia's ranking in the United Nations E-Government Development Index.	2 hours
Critical	A comprehensive impact on the digital platforms and applications provided throughout the Kingdom to include one or two of the following stakeholders: • government agency • Business and Supply Chains • Citizens and Residents	Financial losses of up to 500,000 Saudi Riyals per hour 0.00575% of the total annual financial return from this service (whichever is greater).	It results in the suspension of compliance certificates (local/international) or exposure to legal action and penalties by local authorities for violating the law.	It results in damage and a negative impact on the institution's reputation in local and/or international media outlets towards the institution.	4 hours
Important	A comprehensive impact on the digital platforms and applications provided at the level of one or more regions of the Kingdom by one of the following stakeholders affiliated with these regions: • government agency • Business and Supply Chains • Citizens and Residents	Financial losses of up to 100,000 Saudi Riyals per hour 0.00115% of the total annual financial return from this service (whichever is greater).	It results in issuing a warning notice to suspend compliance certification and requesting clarification for the incident and immediate remediation from regulatory bodies or facing legal accountability by authorities for potential legal violations.	It results in a limited negative impact on the institution's reputation in local media outlets and complaints from stakeholders.	8 hours
Medium	A comprehensive impact on the digital platforms and applications provided at the level of one or more governorates in one of the regions of the Kingdom from one of the following stakeholders affiliated with these governorates: • government agency • Business and Supply Chains • Citizens and Residents	Financial losses of up to 50,000 Saudi Riyals per hour 0.000575% of the total annual financial return from this service (whichever is greater).	It results in issuing a warning notice and a request clarification of the event from regulatory bodies or being alerted by authorities for a low probability of breaking the law	It results in a negative impact on the institution's reputation, leading to complaints from stakeholders without media attention.	12 hours
Low	A comprehensive impact on digital platforms and applications provided at the level of one or more centers or agency (such as A university or institution) in one of Saudi Arabia's governorates from one of the following stakeholders affiliated with these centers: • government agency • Business and Supply Chains • Citizens and Residents	Financial losses of up to 10,000 Saudi Riyals per hour 0.000115% of the total annual financial return from this service (whichever is greater).	It results in issuing a request for clarification from regulatory authorities and does not result in legal violations.	It does not result in significant effects or draw media attention to the institution	24 hours

*In case of varying classification levels among factors, the highest level is considered.
**Recovery time Objectives are subject to continuous review and updating.

11.2 Change Log Table of the Controls of Risk Management and Business Continuity for Digital Government

The table outlines the changes that have been made to the previous version of the controls of Controls of Risk Management and Business Continuity for Digital Government fourth version.

#	Updated Section	Previous Controls in Version 3	Controls After Change in Version 4	Type of Update
1	8. Business Continuity Controls 8.2.1 Analyze the impact of business disruption and assess risks and threats	Control Number: 05-107-60 Control Statement: Classify the level of importance of government platforms and applications and adhering to the targeted recovery times for each level according to the outage impact assessment matrix issued by the Digital Government Authority (DGA) via the digital portal.	Control Number: 05-107-60 Control Statement: Classify the level of importance of government services, platforms and applications and adhering to the targeted recovery times for each level according to Platforms, Applications and Service Classification Matrix issued by the Digital Government Authority (DGA) via the digital portal.	Updated Control
2	8. Business Continuity Controls 8.2.3 Developing Business Continuity Plans	Control Number: 05-107-69.07 Control Statement: Procedures for Recovering Operations and Priority Procedures, Clarifying Internal and External Implications in the Execution Mechanism.	Control Number: 05-107-69.07 Control Statement: The procedures for recovering operations and priority procedures, including alternatives and actions to be taken in the event of a complete digital service outage, along with an explanation of the internal and external dependencies in the implementation mechanism.	Updated Control
3	8. Business Continuity Controls 8.2.4 Develop Disaster Recovery Plans for Information and Communication Technology (ICT)	Control Number: 05-107-71 Control Statement: Determine the main objectives of the Disaster Recovery Plans for Information and Communication Technology (ICT), including appropriations on external suppliers and any outsourced services.	None	Deleted Control
4	8. Business Continuity Controls 8.2.4 Develop Disaster Recovery Plans for Information and Communication Technology (ICT)	None	Control Number: 05-107-71 Control Statement: Providing backup data centers for critical and sensitive platforms and applications within the agency, according to the results of the business impact analysis.	New Control
5	8. Business Continuity Controls 8.2.4 Develop Disaster Recovery Plans for Information and Communication Technology (ICT)	None	Control Number: 05-107-72 Control Statement: Providing backup and alternative communication circuits for the communication lines that serve the agency's critical sensitive systems and services from different service providers, using various technologies.	New Control
6	8. Business Continuity Controls 8.2.4 Develop Disaster Recovery Plans for Information and Communication Technology (ICT)	None	Control Number: 05-107-73 Control Statement: Conducting regular tests for backup and alternative communication circuits to ensure their effectiveness and the continuity of digital services.	New Control
7	8. Business Continuity Controls 8.2.4 Develop Disaster Recovery Plans for Information and Communication Technology (ICT)	None	Control Number: 05-107-77 Control Statement: Providing the availability percentages of the platforms and applications affiliated with the agency to the Digital Government Authority monthly, along with supporting evidence to validate the submitted percentages through "the service for updating the availability rates of digital government services" on Raqmi Portal.	New Control
8	8. Business Continuity Controls 8.2.4 Develop Disaster Recovery Plans for Information and Communication Technology (ICT)	Control Number: 05-107-78 Control Statement: Test and review Disaster Recovery Plans for Information and Communication Technology (ICT) at least once a year or when there is a significant change in the agency's IT infrastructure to ensure its readiness in case of any disruptions.	Control Number: 05-107-81 Control Statement: Testing the Information and Communication Technology disaster recovery plans, including the activation of backup data centers and the restoration of critical and sensitive platforms and applications within the agency at least once a year, or whenever there is a significant change to the agency's IT infrastructure.	Updated Control
9	Appendix	Matrix for Assessing Disruption Impact and Targeted Recovery Time	Platforms, Applications and Services Classification Matrix	• Update the definition of the very critical level for the impact factor on Stakeholder • Update the recovery time objective

هيئة الحكومة الرقمية
Digital Government Authority

DGA.GOV.SA