وزارة النقل والاتصالات وتقنية المعلومات
Ministry of Transport, Communications and Information Technology

Guideline for IT Operations Continuity Policy

April 2026

نصل العالم
Connecting the world

@mtcitoman

Issuance and Distribution:

Issuing Authority	Email:	Issue Date:
General Directorate of Policies and Governance Ministry of Transport, Communications and Information Technology	Governance@mtcit.gov.om	2025

Document Record:

Version	Date	Issuing Authority	Notes
0.1	2018	Information Technology Authority	IT Services Continuity Framework
0.2	2026	Ministry of Transport, Communications and Information Technology	Guideline for IT Operations Continuity

Distribution List

1.	All units of the State Administrative Apparatus
2.	Ministry official website

Table of Contents

1. Introduction

This guideline provides a comprehensive and structured approach to ensuring the continuity of Information Technology (IT) operations across government Units and their contracted partners. it has been developed in alignment with international best practices and globally recognized standards issued by the International Organization for Standardization (ISO).

The guideline aims to support government Units in building resilient, reliable, and effective IT capabilities that enable them to respond efficiently to potential crises and emergency situations that may disrupt IT operations. It focuses on minimizing operational and financial losses, ensuring continuity of critical services, and preserving the Units reputation and the trust of stakeholders and service beneficiaries.

2. Purpose

To provide a systematic framework for managing IT operations continuity during crises and emergency situations.

3. Objectives

- To unify practices and procedures across government Units to ensure compliance with local and international standards.
- To ensure the integration of continuity plans with the operational and technical processes of each Unit
- To define responsibilities and roles related to the continuity of IT operations.
- To enhance the capabilities of government in delivering their services effectively during crises and emergency situations.

4. Scope of implementation

This guide applies to all Units within the state's administrative apparatus and their contracted partners, and it covers all aspects of IT operations continuity, including planning, implementation, testing, review, and continuous improvement.

5. Core Principles

This guide is founded on the fundamental principles outlined in the relevant ISO standards, specifically ISO 22301 (Business Continuity Management), ISO/IEC 27001 (Information Security Management), and ISO/IEC 27031 (Information and Communication Technology Readiness for Business Continuity).

The key principles are as follows:

• Risk Management as Part of IT Operations Continuity

IT operations continuity plans are developed based on the Outcomes of risk assessments and Business Impact Analyses (BIA) to ensure proactive and effective management of potential threats.

• Comprehensiveness and Integration

The plans encompass all elements and processes of IT and critical services, ensuring their alignment and integration with other enterprise Business Continuity Plans (BCPs) to provide a unified and coordinated response during emergency situations.

• Periodic Assessment and Continuous Improvement

The plans are regularly reviewed and updated in light of technological advancements and improvements, changes in services or business processes, and outcomes of tests and drills to ensure their continued effectiveness.

• Clarity of Roles and Responsibilities

The roles and responsibilities of all staff and management levels are clearly defined to ensure a prompt and effective response in any emergency situation.

• Flexibility and Adaptation to Changes

The plans are designed to be adaptable to technological, operational, legislative, and regulatory changes, ensuring the continued effectiveness and continuity of services and critical operations.

6. Contents of the Guidance Manual

The IT operations continuity guide covers the following key topics:

6.1 Roles and Responsibilities by Level

o Senior Management

• Define IT continuity policies and plans and ensuring their alignment with the unit's objectives.
• Approving continuity plans and Allocate the necessary resources for their implementation.
• Reviewing plan test results and periodic reports and take the necessary decisions to enhance continuity.
• Monitoring the commitment of relevant teams and departments to their roles and responsibilities during emergencies.
• Promoting a culture of continuity and raise awareness of the importance of business continuity among all employees.

o Head of IT Operations Continuity Team

• Supervise all IT operations continuity activities and coordinate with senior management to ensure alignment with the organization’s Business Continuity Plans (BCPs).
• Making operational decisions crises and emergency situations and periodically reviewing plan updates.

o Risk Assessment and Business Analysis Officer (BIA & Risk Officer)

• Prioritize critical services, conduct Business Impact Analyses (BIA), and assess IT-related risks.
• Provide recommendations to mitigate risks and ensure IT system readiness

o Disaster Recovery & IT Continuity Officer

• Develop technical emergency and recovery strategies and implement them during tests or actual incidents.

• Identify recovery plans for all critical operations and ensure the readiness of alternative resources.

o Infrastructure & Technical Support Officer

• Manage technical resources and ensure the readiness of IT systems, networks, and servers.

• Provide technical support during the implementation of continuity plans and simulation exercises.

o Communication Officer

Manage internal and external communication channels during emergencies and provide accurate information to relevant authorities.

o Support Team Members

Support the implementation of continuity plans during emergencies and participate in simulation exercises to ensure integrated response and rapid recovery.

6.2. Business Impact Analysis (BIA)

The Business Impact Analysis (BIA) aims to identify critical IT services and systems and assess the impact of their disruption on essential business operations. This includes specifying the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each critical service. The analysis also seeks to evaluate the potential effects of disruptions prioritize recovery activities accordingly. The BIA should include the following:

o Identifying critical services and systems

Identifying all IT services and systems that support critical operations, including:

• A list of all essential processes, systems, and services of the Unit.

• classification of these according to their business criticality and service add requirements.

o Identifying potential impacts

Assessing the potential impacts resulting from the failure of each critical IT service or system. These impacts may add but are not limited to, the following:

• Financial impacts: direct and indirect such as fines, penalties, and recovery costs.

• Operational impacts: Disruption, degradation, or delay in the delivery of critical operational services.
• Legal and regulatory impacts: Non-compliance with applicable laws, regulations, and standards.
• Reputational impacts: Loss of beneficiary trust and adverse effects on the organization's reputation and public image.

o Prioritizing and acceptable downtime duration

Based on potential impacts, recovery objectives are established for each critical IT service or system. These objectives add the following:
• Recovery Time Objective (RTO): The maximum period of time within which an IT service or system must be restored to an acceptable level of operation following a disruption.
• Recovery Point Objective (RPO): The maximum acceptable amount of data loss an organization or unit can tolerate for a specific service or system, indicating how current date the restored data must be.

o Identifying critical resources for operations recovery: personnel, equipment, systems, data, facilities, and communication resources required to ensure restoration of operations.

o Identifying dependencies and interdependencies: recognizing relationships and interdependencies among, services, systems, internal and external parties that may affect service continuity.

o Identifying associated risks and threats:

• Identifying the types of risks that may affect systems, services, and data in accordance with the IT Risk Management Policy and Guide issued by the Ministry of Transport and Information and Communications Technology.
• Assessing the likelihood of each risk occurring and its potential impact

6.3. Continuity Plans

IT continuity plans aim to ensure the continuous operation of a unit's critical systems and services of the unit during crises or emergencies, while minimizing the risks associated with system downtime. These plans are developed based on the results of business

impact analysis and risk assessment, and appropriate strategies are designed to ensure IT operations continuity. These plans must align with the recovery objectives (RTO and RPO) defined in the business impact analysis.

The main continuity plans include the following:

o Backup and Recovery

The backup and recovery plan is considered the cornerstone of any IT business continuity plan, This plan should include the following:

• Identifying critical data and systems: Determine all data, applications, and systems that need to be backed up regularly.
• Backup schedule: Define the frequency of backups (e.g., daily, weekly, monthly) based on the RPO of the data and systems.
• Backup methods: Apply appropriate backup methods (e.g., full, differential, incremental) store backups in secure, geographically separate locations.
• Recovery testing: Regularly test recovery procedures to ensure that data and systems can be successfully restored within the required timeframe.

o Disaster Recovery (DR) Plans

Disaster recovery plans are essential to ensure business continuity in the event that the unit's primary site fails. These plans developed based on RTO and RPO for critical services as well as the available budget. Examples of disaster recovery sites include:

• Hot Sites: Fully prepared sites with all necessary equipment, data, and applications, which can be activated almost immediately.
• Cold Sites: Sites that provide space and basic technical infrastructure (such as power and cooling) but require the installation and configuration off equipment, software, and data.
• Cloud-Based Disaster Recovery Sites: Utilizing cloud services to restore systems quickly and flexibly.

o Resilience and Redundancy

The concept of resilience and redundancy aims to ensure the continuous operation of systems and services without interruption in the event of any failure or malfunction. this approach relies on maintaining additional copies of systems, servers, and communication paths, as well as designing systems capable of rapid and efficient self-recovery, thereby

reducing risks and ensuring reliable and effective business continuity:

• Redundant components: Utilizing redundant components (such as servers, storage devices, network components, and power supplies) eliminate single points of failure.

• Load Balancing: Distributing traffic across multiple servers to increase availability and reduce the load on any single server.

• Multipath networks: Designing networks with multiple paths to ensure continuity of connectivity in the event that one path fails.

o High Availability (HA)

Designing critical systems to operate almost continuously, even in the event of technical failures or issues, aims to minimize downtime and ensure uninterrupted delivery of essential services to beneficiaries and employees through the following mechanisms:

• Designing critical systems for continuous operation: Each critical system is designed to remain permanently available, with the capability to handle technical failures or operational load without service interruption.

• Implementing clustering and synchronous replication methods to ensure continuous operation.

o Outsourcing

The continuity of IT operations may, in some cases, require outsourcing certain critical services. Examples include hosting services, technical support services, and cloud computing services. When this option is adopted, the relevant unit must carefully select service providers based on clear criteria and ensure contracts with them include Service Level Agreements (SLAs) that explicitly define the continuity requirements and recovery plans.

o Communication and Contact Plans

• A detailed communication plan must be prepared between the IT Operations Continuity team and relevant suppliers, including the following elements:

• Maintain up-to-date contact details for each supplier, including direct phone numbers, email addresses, and alternative communication methods for emergencies.

Identify primary and backup contacts within the IT Operations Continuity team and the relevant suppliers, documenting their names and positions.

• Establish a clear escalation procedure in case communication through primary channels fails.
• Define response timeframes and outlining the responsibilities of each party during outages or the recovery phase.

6.4. Testing and Exercises

IT operations continuity plans should be tested regularly to ensure their effectiveness and to identify any gaps or deficiencies before an actual incident occurs. Testing can include tabletop exercises, simulation tests, and full-scale tests. These activities help train teams, improve procedures, and verify that the defined in the Business Impact Analysis (BIA) can be achieved. Types of tests and exercises include:

o Walk-through Tests

Walk-through tests involve reviewing IT operations continuity plans in coordination with the relevant teams to discuss the procedures in place, address any areas that need clarification or alignment, and ensure that all parties clearly understand their roles and responsibilities.

o Simulation Tests

Simulation tests replicate a specific incident in a controlled environment. Relevant portions the plan is activated, and the corresponding teams carry out the prescribed procedures. These tests allow for evaluating the effectiveness of the procedures, identifying weaknesses in the plan, and training teams to respond in a realistic environment.

o Parallel Tests

Parallel tests involve running normal operations at the primary site while simultaneously activating at the alternate site. Live or replicated data is used to assess the alternate site's ability to support operations without impacting ongoing operations.

o Cutover Tests

Cutover tests involve transferring actual operations from the primary site to the alternate site. This is the most comprehensive and realistic type of test; however, it carries higher risks as operations at the primary are temporarily halted.

o Documentation and Post-Test Review

• After each test or exercise, the results must be accurately documented, the following:
• The tested scenario.
• The teams involved.
• The observed results.
• Lessons learned.
• Recommendations for improvement.

6.5. Performance Indicators and Continuous Improvement

Continuous improvement is a fundamental component in ensuring the effectiveness and sustainability of IT operations continuity plans. This approach is based on periodic evaluation and systematic enhancement of plans and procedures, ensuring their alignment with technological, organizational, and operational changes. This is achieved through the following:

• Periodically reviewing and updating plans and procedures based on organizational, technical, and operational changes, as well as lessons learned.
• Conducting tests and simulation exercises to measure readiness, response efficiency, and to identify and correct deficiencies.

• Analyzing lessons learned from incidents and past experiences to improve future performance.
• Updating risk assessments and Business Impact Analysis (BIA) to identify emerging threats and adjust priorities accordingly.
• Enhancing human and organizational readiness through continuous training and awareness programs.
• add the technical infrastructure by adopting supporting technologies such as backup solutions and cloud-based recovery.
• Monitoring performance indicators to evaluate implementation effectiveness and identify proactive improvement opportunities.

7. Integration

~~The~~ integration between IT risk management and IT operations continuity is essential and necessary to ensure the protection and continuity of critical services and operations. The risk management guide provides the foundation for understanding threats, assessing risks, and developing mitigation plans, while IT Operations Continuity Guide translates these assessments into practical plans that ensure the continuity of critical operations and services as well as recovery of systems and services during crises and emergencies.

8. Document Management

This guideline is owned by the Ministry of Transport and Communications and Information Technology and will be subject to revision whenever necessary.

9. References

- ISO 22301:2019 – Business Continuity Management Systems
- ISO/IEC 27001:2022 – Information Security Management Systems
- ISO/IEC 27031:2025 – ICT Readiness for Business Continuity
- ITIL 4

Appendix 1: Terms and Definitions

Ministry	Ministry of Transport, Communications and Information Technology
IT Operations	It is a set of organized activities and procedures responsible for managing, operating, and maintaining IT infrastructure and the related services, ensuring service continuity, availability, and performance of services in line with business and end-user requirements. these operations typically include network, server, database, and application management, as well as cybersecurity, backup and recovery, and continuous monitoring of system performance and incidents.
Risk	The likelihood of unexpected events or circumstances arising from threats or vulnerabilities in systems, processes, or technical resources, which may negatively affect the confidentiality, integrity, or availability of information, or impact business continuity and the achievement of operational and organizational objectives.
Backup	Perform regular backups of data and systems to ensure business .continuity in the event of system failures or data loss
Audit	Reviewing activities and system changes to potential deviations, non-compliance, or security breaches.
Periodic Reviews	Periodic evaluation of controls and procedures to ensure their effectiveness and their alignment with changes in the work environment and emerging risks
Recovery Time Objective (RTO)	It is the maximum allowable duration that operations or services can be halted following a crisis or emergency, that is, the time within which operations must be restored to normal or an acceptable level of service.
Recovery Point Objective (RPO)	The maximum allowable data loss in the event of an outage or emergency, that is the point in time before which data must be recovered to avoid impacting the unit's critical operations.

Business Impact Analysis (BIA)	It is a systematic process of identifying a unit's critical services and processes, assessing the potential impacts of their disruption, and determining the time priorities and resources required for their recovery, the goal is to support strategic decision-making in IT operations continuity.
Alternative Resources	All sites, equipment, systems, data, communication methods, and backup personnel that may be utilized to ensure the continuity of the unit's critical services in the event of any disruption or emergency.
Full Backup	The process of creating complete backups of all critical data and systems on a regular basis
Differential and Incremental Copies	Copying only the changes made since the last full or incremental backup in order to reduce the amount of data copied and speed up the restoration processes.
Multi-Site Storage	Storing backups in multiple secure locations, including onsite, offsite, and cloud environments.
Assembly	Connecting a group of servers so that they operate as a single unit; if one server fails, the others automatically its tasks without service interruption.
Synchronous replication	Continuously copying data between multiple servers that ensure backup copies are immediately available when needed
Emergency events	An unplanned service outage or degradation in service quality, where the objective is to restore the service to its normal state as quickly as possible in order to minimize the impact on add operations.

Information Technology Continuity Plan	A systematic and comprehensive document that outlines the procedures, plans, and measures necessary to ensure the continuous operation of critical information services, systems, and technologies during emergencies or disruptions, and to enable ~~the~~ restoration of services to acceptable levels within the targeted time frame (RTO).

Appendix 2: Business Impact Analysis (BIA) Template

General Information

- Unit/Department Name:
- Person Responsible for Analysis:
- Date of Analysis:
- Scope of Analysis:

o Systems:

o Processes:

o Critical Services:

Identifying vital processes

Transaction number	Operation Name	Objective / Purpose	Description	Operations Manager	Repeat the process	Notes
1						
2						
3						

Business Impact Assessment

The operation	Category	Financial impact	Operational impact	Impact on reputation	Legal Impact / Compliance	Total Score
	Low / Medium / High					
	Low / Medium / High					
	Low / Medium / High					

Defining business continuity requirements

The operation	Maximum Tolerable Period of Disruption (MTPD)	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)	Required resources

Assessment of the risks associated with each process

The operation	Potential risks	Probability	Impact	Proposed Response Plan
		Low / Medium / High	Low / Medium / High	
		Low / Medium / High	Low / Medium / High	
		Low / Medium / High	Low / Medium / High	

Priorities and Recommendations

- Prioritize processes based on their importance and business impact.
- Recommend continuity measures for each critical process.
- Identify alternative resources or required technical solutions.
- Periodically update the plan to reflect operational changes.

Analysis Outputs

A list of critical processes with their respective priorities.

- RTO and RPO defined for each process.
- Business continuity requirements for each system and its resources.
- Recommendations to improve preparedness and minimize the impact of disruptions.

Appendix 3: IT Operations Continuity Plan Test

General Information

- Unit/Department Name:
- Person Responsible for the Test:
- Planned Test Date:
- Actual Test Date:

Test Type

- Tabletop Exercise
- Partial Test
- Full-scale Test

Test Objectives

- Evaluate the effectiveness of the business continuity plan.
- Identify gaps in procedures, processes, and resources.
- Assess the readiness of personnel, teams, and supporting technologies.
- Revise the plan based on test results and lessons learned.

Test Scope

Component	Coverage	Notes
Critical Systems	✓ / ✗	
Data	✓ / ✗	
Human Resources	✓ / ✗	
Networks & Communications	✓ / ✗	
Alternative Facilities	✓ / ✗	

Proposed Test Scenarios

Scenario No.	Incident Type	Brief Description	Affected Systems	Test Objective
1	Power Outage	Loss of power at primary data center	Servers & Networks	Validate alternate site response
2	Data Loss	Corruption of primary database	Database Systems	Test data recovery from backups
3	Cybersecurity Incident	Cyberattack	All Systems	Test security and recovery procedures
4	Natural Disaster	Flood / Fire	Critical Facilities	Test emergency relocation plans

Test Steps

1. Announce the start of the test to all participating teams.
2. Execute the test scenario according to the planned type.
3. Record observations during the test, including response times, issues encountered, and effective actions taken.
4. Measure performance against defined RTO and RPO.
5. Collect feedback from all participating teams.
6. Prepare a lesson's learned report summarizing findings and recommendations.

Test Performance Indicators

Indicator	Target	Actual Measurement	Comments / Corrective Actions
System Recovery Time	≤ RTO		
Data Loss	≤ RPO		
Successful Procedure Rate	≥ 90%		
Team Readiness	100%		
Availability of Alternative Resources	100%		

Recommendations after the test

- Revise the business continuity plan to address identified gaps.
- Retrain personnel and teams on missing procedures.
- Review contracts with alternative service providers, if required.
- Retest critical elements within 6 months.

Appendix 4: Actual Performance Indicators Model for the IT Business Continuity Plan (IT Business Continuity KPIs)

Indicator	Description	Planned Goal/Standard	Actual Measurement	Comment / Corrective Actions
(Actual Recovery Time)	Actual time taken to restore the system after an incident	≤ Planned RTO for each system	Example: 3 hours versus planned RTO of 2 hours	If it exceeds the actual, review recovery procedures or improve infrastructure
Deviation from RTO (%)	The percentage difference between actual time and planned RTO	≤ 10%	Example: 50% increase over the planned RTO	Analysis of delay causes and updating recovery plans
(Annual Test Execution Rate)	The percentage of scheduled tests that were actually conducted	100%	Example: 80%	Setting a new schedule for delayed tests and documenting the lessons learned
Business Continuity Test Success Rate (%)	The percentage of tests that achieved the specified objectives	≥ 90%	Example: 85%	Improving recovery procedures and correcting failure points
IT Systems Business Continuity Plan Coverage	Percentage of critical systems that have a continuity plan	100%	Example: 95%	Completing plans for uncovered systems
Team response time to crises and emergencies	Actual response time to interruption or malfunction	≤ 30 minutes	Example: 45 minutes	Additional training for the team and improving early warning mechanisms

(Incident Response Time)				
Number of incidents that exceeded RTO/RPO	The number of incidents that have not been recovered within the planned frameworks	0	Example: 2 emergency cases	Review the plan for each system and ensure the readiness of the infrastructure
Repeated updating of continuity plans	Number of times continuity plans were updated in the year	≥ 1 annual update	Example: Only once	Develop a periodic review plan and improve coverage