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

Guidelines for IT Risk Management Policy

February 2026

نصل العالم
Connecting the world

@mtcitoman

Issuance and Distribution:

Issuing Authority	E-mail	Issue Date
General Directorate of Policies and Governance Ministry of Transport, Communications and Information Technology	Governance@mtcit.gov.om	2026

Document Control:

Version	Date	Issuing Authority	Comments
0.1	2026	Ministry of Transport, Communications and Information Technology	

Distribution List	
1	All State Administrative Apparatus units

Contents:

Introduction:

Information Technology Risk Management is considered one of the fundamental pillars for maintaining the integrity and security of digital assets within government units. This guide aims to provide a comprehensive and systematic framework that enables the early identification and assessment of risks associated with information technology, followed by the implementation of appropriate preventive measures to mitigate their impact on business operations.
The guide also seeks to enhance institutional awareness of the importance of technological risks and to raise the level of preparedness in addressing and managing such risks effectively

Objectives:

1. Clarifying the methodology for implementing the Information Technology Risk Management Policy.
2. Ensuring alignment with international standards, best practices, and recognized models in the field of risk management.
3. Developing effective strategies and procedures for risk mitigation and treatment.
4. Protecting the confidentiality, integrity, and availability of data and digital assets.
5. Supporting risk-based decision-making to improve operational and strategic performance.

Purpose:

Providing a practical guidance manual that contributes to the effective implementation of Information Technology Risk Management within government units, while enhancing institutional readiness for rapid response to security incidents and ensuring service continuity.

General Principles:

The Risk Management Policy shall be applied within the covered units based on the following principles:

1. **Integration:** Risk management shall be integrated into the Information Technology strategy of the entity.

2. **Proactiveness:** Risk management shall be practiced in a preventive manner to mitigate potential impacts before risks materialize.
3. **Objectivity:** Risks shall be assessed based on objective analysis supported by accurate and reliable data.
4. **Proportionality:** Controls and procedures shall be determined in proportion to the level of risk.
5. **Continuous Improvement:** Risk management processes shall be periodically reviewed and continuously updated to ensure their effectiveness and alignment with evolving changes.

Governance Structure of the Guidance Manual

1.Definition of Roles and Responsibilities

- **Senior Management:**

  - Approve the Risk Management Policy and oversee its implementation.
  - Allocate the necessary resources for effective risk management.
  - Review risk reports and take required strategic decisions.
  - Ensure the entity maintains institutional awareness of the importance of risk management.
  - Designate an official point of contact with national authorities responsible for cybersecurity and IT risk.

- **Risk Management Team**

  - Responsible for continuously identifying, assessing, and categorizing IT-related risks.
  - Responsible for developing response plans and risk mitigation procedures.
  - Ensure the implementation and monitoring of risk management controls and techniques.
  - Prepare and submit periodic reports to senior management on the status of risks and the actions taken.

- **IT Team**

  - Responsible for implementing the recommended technical controls to address identified risks.
  - Responsible for monitoring systems and applications to detect any vulnerabilities or threats.
  - Support the technical assessment of cybersecurity incidents.

RACI Matrix – Information Technology Risk Management

Activity / Responsibility	Risk Management Team	IT Teams	Senior Management	Relevant National Authorities
Identify and assess risks	R (Responsible)	C (Consulted)	I (Informed)	-
Develop risk mitigation plans	R (Responsible)	C (Consulted)	I (Informed)	-
Implement technical controls	C (Consulted)	R (Responsible)	I (Informed)	-
Monitor incidents and threats	C (Consulted)	R (Responsible)	I (Informed)	-
Escalate critical risks	R (Responsible)	C (Consulted)	R (Responsible)	-
Take strategic decisions	I (Informed)	I (Informed)	R (Responsible)	-
Coordination with relevant national authorities	I (Informed)	I (Informed)	C (Consulted)	R (Responsible)

2.Mechanisms for Reporting High-Priority Risks

1. **Establish a clear risk classification mechanism** to prioritize risks based on their impact and likelihood of occurrence.
2. **Implement an internal reporting system** for critical risks (e.g., an electronic platform or standardized reporting forms) to notify relevant authorities within the entity immediately.
3. **Define escalation levels**, starting from the Risk Management Team, through IT Teams, up to Senior Management and the relevant national authorities.
4. **Adopt standardized templates and reports** for documenting and evaluating risks and the actions taken.

Risk Escalation and Reporting Procedures Form

Report No.	Report Date	Risk Description	Risk Severity Level	Mitigation Actions Taken	Responsible Department	Response Date	Current Status
1	12-Aug-2025	Compromise of the email system	Critical	System isolation and mandatory password reset implemented	Information Technology Department	12-Aug-2025	In Progress
2	11-Aug-2025	Delay in applying security system updates	Medium	Immediate scheduling and execution of required updates	Risk Management Department	12-Aug-2025	Completed
3	10-Aug-2025	Loss of unclassified data	High	Data restored from approved backup sources	Information Technology Department	11-Aug-2025	Under Review

3. Coordination Mechanisms with Relevant National Authorities

- Exchange of information and reports related to security threats and technological risks.
- Participation in national initiatives, awareness programs, and training activities to enhance institutional capabilities.
- Compliance with relevant national requirements and regulations, and ensuring that policies and procedures are updated in accordance with governmental directives.

4. Classification of Technical Assets

4.1 Technical Asset Categories

- **Physical Assets (Hardware):**
  Includes computers, servers, networking devices, storage units, and communication equipment.
- **Software Assets (Software):**
  Includes operating systems, enterprise applications, middleware, and software tools.
- **Data (Data):**
  Includes databases, electronic files, sensitive information, and customer data.
- **Network (Network):**
  Includes network infrastructure, routers, firewalls, and access points.
- **Technical Services (Services):**
  Includes hosting services, cloud services, managed databases, and technical support services.

4.2Technical Asset Classification Criteria

The classification of technical assets is based on the following criteria:

- **importance:** The extent to which the loss, damage, or unavailability of the asset may impact the continuity and effectiveness of business operations.
- **Sensitivity:** The level of confidentiality and sensitivity of the information or data associated with the asset, requiring protection against unauthorized access.
- **Replaceability:** The degree of difficulty in replacing, restoring, or recovering the asset in the event of loss or damage.
- **Reliability:** The reliance of critical business processes on the asset and the potential operational impact in case of failure.
- **Financial Value:** The monetary value of the asset, including acquisition, maintenance, and replacement costs.

Technical Asset Classification Levels Form

Category	Description	Examples
Critical Assets	Assets that directly affect business continuity and the security of sensitive data.	Electronic payment systems, customer databases
Sensitive Assets	Assets containing confidential information that require a high level of protection.	Employee data, sensitive internal applications
Important Assets	Assets that support core operations but are less sensitive.	Core servers, production software
Standard Assets	Assets with low impact on business operations and that do not contain sensitive information.	General desktop computers, standard software

4.3 Practical Steps for Classifying Technical Assets

1. **Asset Inventory:**
   Prepare a comprehensive list of all technical assets within the unit.

2. **Asset Assessment:**
   Evaluate each asset according to the established criteria (importance, sensitivity, financial value).

3. **Classification Assignment:**
   Assign each asset to its corresponding classification category.

4. **Documentation of Results:**
   Create a centralized record of asset classifications with periodic updates.

5. **Implementation of Security Controls:** Determine and apply appropriate security measures for each asset category based on its classification level.

Technical Asset Inventory and Classification Form

Asset No.	Asset Name	Asset Type	Brief Description	Financial Value	Sensitivity (Low, Medium, High)	Importance (Critical, Important, Standard)	Location / Department	Asset Owner	Controls / Procedures
001	Database Server	Hardware/ Software	Server hosting customer database	OMR 50,000	High	Critical	Data Center	IT Team	Requires high protection
002	Attendance & Payroll Application	Software	Internal system for employee attendance management	OMR 10,000	Medium	Important	HR Department	System Manager	Monthly updates
003	Internal Internet Network	Network	LAN connecting all company devices	OMR 30,000	Medium	Important	Network Center	Network Administrator	Regular maintenance

5. Risk Management Methodology

1. Identification of Technical Assets: Select the assets targeted for analysis based on the results of the asset inventory and classification.
2. Identification of Threats and Vulnerabilities:
    - Enumerate potential threats (e.g., cyberattacks, system failures).
    - identify vulnerabilities in the assets (e.g., outdated patches, misconfigurations).
3. Risk Analysis:
    - **Qualitative:** Assess the likelihood and impact based on the expertise of the responsible teams.
    - **Quantitative:** Estimate potential losses numerically, whether financial or operational.
4. Risk Assessment and Prioritization
    - Use a risk matrix to determine the severity and likelihood of each risk (Impact vs. Likelihood).
    - Classify risks into the following levels: Low – Medium – High – Critical.
5. Risk Treatment
    - **Mitigation:** Reduce the likelihood or impact of the risk.
    - **Transfer:** Shift the risk to another party or through insurance.
    - **Acceptance:** Accept the risk if it falls within the acceptable level.
    - **Avoidance:** Discontinue the activity that generates the risk.
6. Approval and Oversight
    - Senior Management Approval of Assessment Results and Risk Treatment Plan: Ensure that the risk assessment outcomes and the proposed Risk Treatment Plan are formally approved by senior management.

- Assignment of Implementation and Monitoring Teams: Designate responsible teams to execute the risk treatment measures and continuously monitor their effectiveness.

7. Continuous Monitoring and Review: Conduct periodic reviews of risks and update the risk assessment whenever changes occur.
8. Documentation and Reporting
    - Maintain all results in a centralized risk register
    - Prepare periodic reports and submit them to senior management.

6. Control and Protection Measures

Control and protection measures for assets are an essential part of risk management to ensure their protection and to reduce the likelihood or impact of risks. These measures are divided into three main types:

6.1Technical Controls

- **Data Encryption**: Encrypt data during storage and transmission to ensure confidentiality and integrity.
- **access and User Rights Management:** Control access and user permissions, including the use of multi-factor authentication.
- **Regular Data and System Backup:** Perform periodic backups of data and systems to ensure business continuity.
- **Network Segmentation:** Isolate sensitive systems and services to reduce impact in the event of a security breach.

6.2 Administrative / Procedural Controls

- **Periodic Audits:** Conduct regular audits of system activities and changes to ensure compliance with policies and procedures.

- **Controls and Procedures Review:** Periodically review controls and procedures to verify their effectiveness and alignment with changes in the work environment and emerging risks.

6.3Supplier and Contractor Controls

- **Inclusion of Security Requirements in Contracts**: Include clear security requirements and controls in contracts and agreements with suppliers and contractors.
- **Periodic Supplier and Contractor Assessment**: Regularly evaluate suppliers and contractors to verify their compliance with security controls.
- **Monitoring Supplier Activities**: Track and monitor activities performed by suppliers to ensure they do not compromise the security of data and systems.

7. Integration with Business Continuity

he integration of risk management with business continuity and disaster recovery plans aims to ensure the unit's readiness to handle emergency events and minimize their impact on critical operations. This includes:

- **Incorporating Risk Assessment Results into BCP/DRP Plans:** Identify critical assets and vital operations and ensure their protection based on the outcomes of risk assessments.
- **Aligning Measures Between Risk Management and Continuity Plans:** Coordinate procedures such as backups, geographic redundancy (secondary or alternative sites), and recovery points.
- **Defining Shared Responsibilities:** Assign joint responsibilities to risk management, business continuity, and IT teams to ensure a coordinated response.
- **Conducting Periodic Simulation Tests:** Perform regular simulations (annually or semi-annually) of events such as sudden outages or cyberattacks, and update plans based on results to address any identified

Risk Matrix vs. BCP/DRP Measures Form

Risk Type	Impact on Business	Risk Level	Preventive Measures (BCP)	Recovery Measures (DRP)	Responsible Team
Email Compromise	Disruption of internal communication	Critical	- Daily email backups- Monitor email for suspicious activity- User training	- Restore system from backups- Change passwords- Activate alternative communication plan	IT Team
Power Outage	Servers and applications downtime	High	- UPS units for all servers- Backup generator- Continuous monitoring of power supply	- Activate backup generator- Shift critical operations to alternative data center	IT Team
Loss of Sensitive Data	Breach of confidentiality, impact on operations	High	- Data encryption- Periodic backups and offsite storage- Access management policy	- Restore from backups- Notify senior management- Review causes and update procedures	IT Team
DDoS Attack	Service disruption or performance degradation	High	- Advanced firewalls- Network traffic monitoring- DDoS protection plans	- Activate emergency response plans- Use external protection services or backups	Cybersecurity Team
Critical System Failure	Disruption of core operations	Critical	- Regular system maintenance- Software and application updates- Continuous system testing	- Activate alternate systems- Restore data and settings	IT Team
Network Outage	Disruption of communications and network-dependent systems	High	- Use alternative network- Reschedule critical activities	- Restore systems from backups- Restart servers	Infrastructure / IT Team
Critical Application Failure	Disruption of application-dependent processes	Medium	- Periodic application testing- Reroute processes to alternative applications- Temporary manual operation plans	- Reinstall applications- Restore data from backups- Test functionality after recovery	IT Team

Natural Disasters	Complete disruption of operations and infrastructure	Critical	- Relocate operations to alternative sites- Ensure employee readiness	- Restore infrastructure- Transfer data and equipment- Activate backup site	Emergency Management / IT Team

8. Monitoring and Continuous Improvement

8.1 Risk Register Review and Update

- **Conduct Periodic Reviews:** Perform regular reviews (e.g., quarterly) to ensure that new or modified risks are correctly assessed and classified.
- **Update the Risk Register:** Add any new risks or revise the assessment of existing risks due to changes in infrastructure, operations, or the technical environment.
- **Document Changes:** Record all modifications or additions, specifying the person responsible for the update and the date of the change.

8.2 Controls Improvement

- **Review Past Incidents:** Analyze previous incidents to identify weaknesses.
- **Update Controls:** Modify technical and procedural controls, introduce new protective tools, and enhance backup procedures.
- **Evaluate and Document Effectiveness:** Assess the effectiveness of updated controls and document results to ensure that the likelihood and impact of risks are reduced as planned.

9. Reporting and Documentation

9.1 Establishment of a Centralized Risk Register

- **Collect All Identified Risks:** Compile all identified risks, assessment results, and treatment plans in a centralized system or table that is searchable and suitable for analysis.

- **Ensure Regular Updates:** Keep the register up to date after each review or whenever a new risk is added.
- **Enable Access for Relevant Teams:** Allow authorized teams to access the register to make informed and timely decisions.

9.2 Periodic Reporting

- **To Senior Management:** Provide summarized reports including risk levels, actions taken, and any critical risks requiring leadership attention.
- **To Regulatory Authorities:** Supply required data in accordance with national regulations, such as the unit's compliance with cybersecurity and risk management standards.
- **Reporting Frequency:** Monthly, quarterly, and annual reports depending on the size of the unit and the sensitivity of the assets.

9.3 Documentation of Treatment and Response Actions

- **Record All Steps:** Document all technical and procedural steps taken to treat each risk, including any related evidence and supporting documents.
- **Ensure Traceability:** Make sure every action is traceable and reviewable to guarantee transparency and compliance with policies.
- **Standardized Templates:** Prepare ready-to-use procedure templates for each type of risk to facilitate consistent documentation across teams.

Document Management

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

Related Documents

- **ISO/IEC 27001:2022** – Information Security Management Systems (ISMS)
- **ISO/IEC 27005:2018** – Information Security Risk Management
- **ISO 22301:2019** – Business Continuity Management Systems (BCMS)
- **ISO 31000:2018** – Risk Management Guidelines
- **NIST SP 800-30 Rev.1 (2012)** – Guide for Conducting Risk Assessments
- **NIST SP 800-37 Rev.2 (2018)** – Risk Management Framework for Information Systems and Organizations
- **COBIT 2019 Framework** – Governance and Management Objectives for Enterprise IT
- **National Data Governance and Management Framework 2025 – Ministry of Transport and Communications**

Appendix: Terms and Definitions

Term	Definition
Ministry	Ministry of Transport, Communications, and Information Technology
Risk	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 the continuity of operations and achievement of organizational objectives.
Risk Management	A systematic process for identifying, analyzing, evaluating, treating, monitoring, and reviewing risks, aimed at reducing their potential negative impact on individuals, assets, systems, or operations, and enhancing the ability to achieve organizational objectives effectively and efficiently.
Critical Systems	Technical or information systems whose disruption, compromise, loss, or misuse can cause severe impacts on business continuity, human safety, national security, delivery of critical services, or regulatory compliance.
Sensitive Systems	Technical or information systems that contain, process, or transmit data requiring special protection due to its sensitivity or nature, such as personal, financial, or health data, or any information that, if disclosed, altered, or accessed without authorization, could cause legal, regulatory, or operational harm.
Ordinary Systems	Technical or information systems that do not contain sensitive or confidential information and are not relied upon for critical operations or delivery of vital services. Exposure to risks for these systems results in limited impact, manageable without significant effect on business continuity, security, or regulatory compliance.
Qualitative Analysis	A risk assessment process that relies on non-numerical methods, focusing on describing, classifying, and relatively estimating the likelihood and impact of risks using descriptive or reference scales (e.g., low, medium, high) to prioritize risk responses.
Quantitative Analysis	A key tool in IT risk management aimed at providing precise numerical estimates of the probability and financial impact of risks, using mathematical and statistical methods to support decision-making regarding treatment priorities and resource allocation.
Risk Register	An official document maintained by the unit that records all identified risks, their analysis, and treatment plans.
Critical Risks	Risks that may result in the disruption of national services or threaten national cybersecurity.

Technical Controls	Technical measures and tools applied directly to systems and assets to protect them.
Encryption	Protecting stored and transmitted data using strong cryptographic techniques to ensure confidentiality and data integrity.
Access Control	Defining and regulating who can access data and systems, including permissions management and multi-factor authentication.
Backup	Performing regular data and system backups to ensure business continuity in case of system failures or data loss.
Network Segmentation	Dividing networks and isolating sensitive systems to reduce the impact of attacks or failures on other assets.
Procedural Controls	Policies and procedures implemented to ensure compliance with security standards and oversight of activities.
Audit	Reviewing activities and system changes to identify any deviations or potential breaches.
Periodic Reviews	Regular evaluation of controls and procedures to ensure their effectiveness and alignment with changes in the work environment and risks.
Technical Assets	All digital resources and technical components used by the unit to support its operations, including hardware, software, data, networks, and digital services.