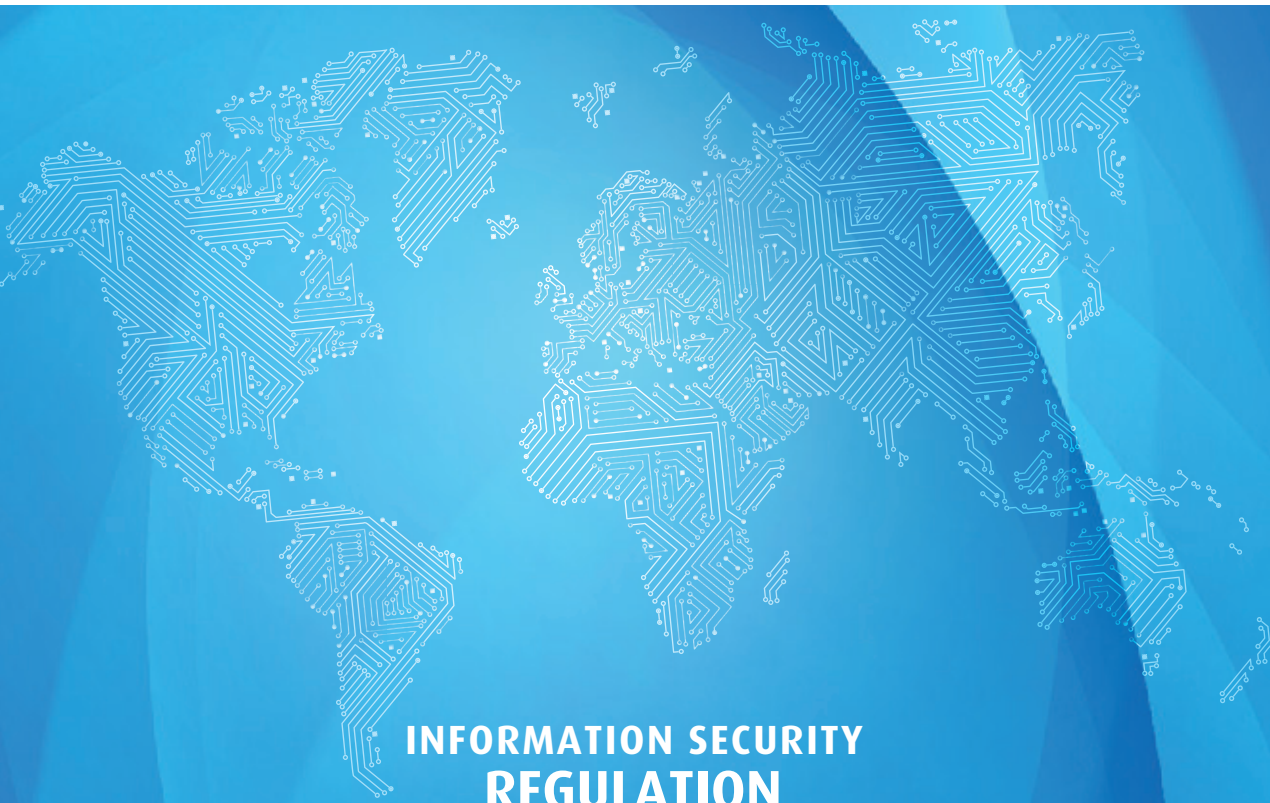
حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER



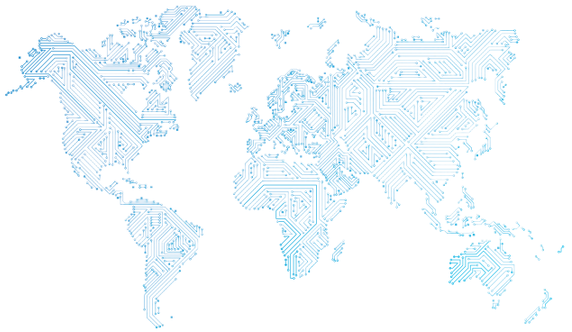
INFORMATION SECURITY REGULATION

VERSION **2.0**

INFORMATION SECURITY REGULATION

Version 2.0

Dubai Electronic Security Center

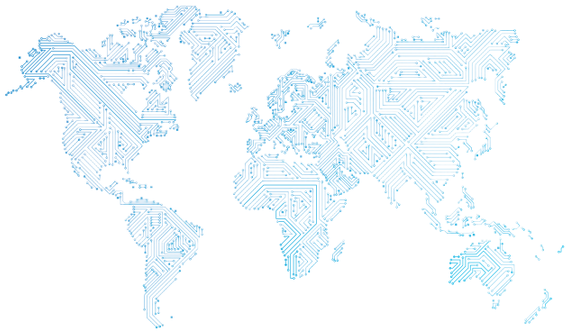


ACKNOWLEDGMENT

The Dubai Electronic Security Center (DESC) has updated The Dubai Government Information Security Regulation (ISR) pursuant to the Dubai Law No. 11 of 2014 and resolution No. 13 of the year 2012 issued by the Chairman of the Dubai Executive Council about Dubai Government's Information Security Regulation. The ISR encompasses several information security domains composed of specific controls and sub-controls, and is closely aligned with other International Information Security related Standards reflecting Dubai Government's acknowledgement and recognition of the information security best practices stated therein. The ISR has also included distinctive items reflecting specific requirements within the context of The Dubai Government. Dubai Electronic Security Center would like to explicitly acknowledge and thank the team members who worked in revising the ISR within The Dubai Electronic Security Center, and various Dubai Government entities, which were consulted during the ISR revision. Dubai Electronic Security Center conducted the final review of the ISR and approved it.

Yousuf AlShaibani
Director General
Dubai Electronic Security Center

TABLE OF CONTENTS



1 INTRODUCTION

Modern social and economic activities are increasingly reliant on information processing. Individuals, communities, public and private sector organizations utilize information in their interactions. Information and Communication Technologies (ICT) based information processing and the already existing non-electronic forms have significantly enhanced the quality of life and the well-being of societies. Electronic services enabled by advances in ICT have become conspicuous among individuals, businesses and government entities tangibly reducing costs and saving time. These advances have also enhanced the economic prosperity, which currently depends to a large extent on technology. Yet, challenges remain for ensuring resilience in dealing with risks which threaten information security. Thus, the need for preserving information security is gaining increasing importance. A secure and trusted information processing environment greatly enhances consumer benefits, business performance, productivity and national security. Conversely, an insecure environment creates the potential for serious damage to organizations (and their vital assets) which could significantly undermine consumers' and citizens' trust. The stakes are particularly high for entities engaged in critical activities, such as public governance, electrical power generation, financial transactions, healthcare services, etc.

The Dubai Government Information Security Regulation provides key practices in information security to be adopted by all Dubai Government Entities (DGEs). It is designed to encourage the employees to adopt information security best practices and ensure the deployment of effective techniques to respond to information security incidents. In addition, the objective of this regulation is to establish an information security culture in all Dubai Government Entities. This culture will encourage Dubai Government Entities to integrate information security within their existing and future strategies.

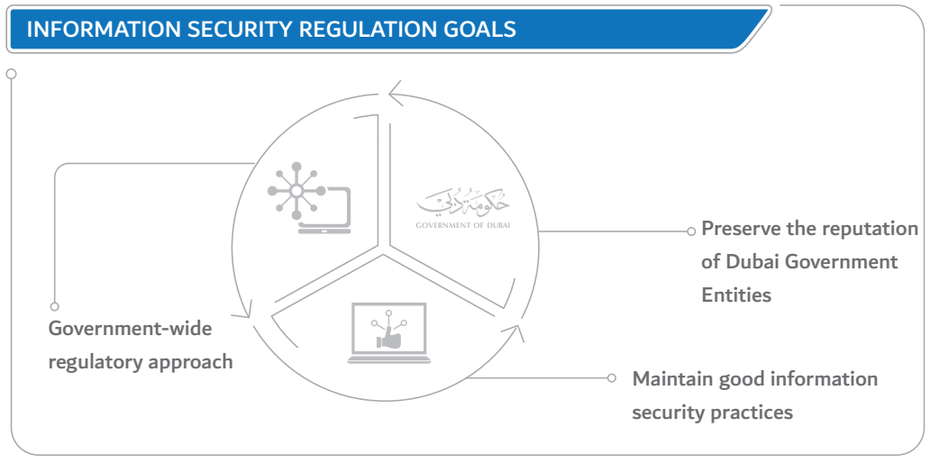
2 PURPOSE

The purpose of the Information Security Regulation is to provide all Dubai Government Entities with the standards to ensure continuity of critical business processes, and minimize information security related risks and damages by preventing and/or minimizing information security incidents. It intends to ensure appropriate level of Confidentiality, Integrity and Availability for information handled within Dubai Government Entities.
The goals of the Information Security Regulation are as follows:

A. To establish a Government-wide regulatory approach to information security

B. To prescribe high-level mechanisms that help identify and prevent information security compromises in order to preserve the reputation of Dubai Government Entities

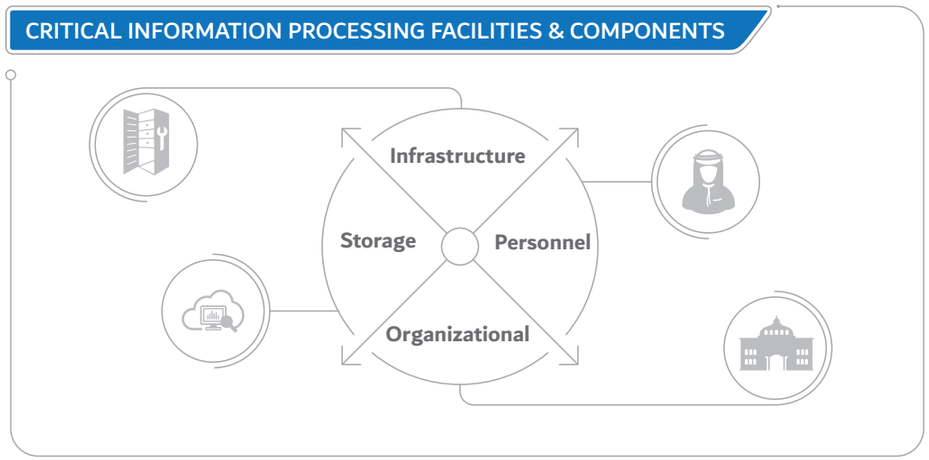
C. To identify the responsibilities required to maintain good information security practices



The Information Security Regulation is a technology neutral framework and will not handle any technological implementation. Therefore, technology specific aspects for implementation will be tackled by Dubai Government Entities reflecting specificities in their internal systems. Dubai Government Entities will be expected to produce a set of policies and procedures that govern their operations in alignment with this regulation. Accordingly, an information security program/management system must be established, implemented and maintained within each Dubai Government Entity.

3 SCOPE

The Information Security Regulation presents the minimum requirements for information security controls and is applicable to all Dubai Government Entities, including but not limited to employees, consultants, contractors and visitors who are not government employees but are engaged with it through various means. Furthermore, the regulation applies to any government information regardless of its type and medium (e.g. Printed, Electronic and Non-Electronic Verbal, Written, etc.). Therefore, Dubai Government Entities are expected to implement this regulation in all the divisions/departments within an entity and not to limit the implementation to Information Technology (IT) divisions/departments only.



The scope of the information security management program must consider all business processes and critical information processing facilities and components, including:

A. Storage (electronics storage device; logical and physical, paper documents, etc.)

B. Infrastructure (hardware, applications, networks, etc.)

C. Organizational (processes, policies, etc.)

D. Personnel (administrators, employees, visitors, etc.)

4 DUBAI GOVERNMENT INFORMATION OWNERSHIP

Dubai Government holds complete ownership of all information processed by all Dubai Government Entities. All Dubai Government employees may conduct various information processing activities based on business requirements and may even temporarily act as owners and/or custodians of information on behalf of their respective entities provided that they are granted corresponding appropriate authorizations. Such information processing authorities are defined by Dubai Government Entities and must be consistent with their mandates and applicable laws & regulations (in line with ISR Ref. 11.1 and 11.2). Safeguarding information is of high priority in order to preserve individual rights and privacy.

Any processing of Personally Identifiable Information (PII) and classified information must be lawful, fair, relevant and not excessive in relation to the purposes for which they are processed. Such purposes should be explicit, legitimate and determined before the time of collection. Dubai Government Entities may at their discretion (ISR Ref.6.5) and in line with applicable laws & regulations (ISR Ref. 11.1 and 11.2), share and transfer information with other Government Entities for the purposes of availing services to the public and businesses (even if the disclosure was not anticipated at the time of information collection) or for their internal administration.

5 INFORMATION SECURITY REGULATION OWNERSHIP AND REVISION

The ownership of this Information Security Regulation belongs to Dubai Government, according to the article number (14) of Dubai Government Executive Council Resolution Number (13) issued in Year 2012. Dubai Government reserves the right to revise the Information Security Regulation in line with changing business needs and Dubai Government priorities in due course as stipulated in the aforementioned resolution.

6 INFORMATION SECURITY REGULATION COMPLIANCE

All Dubai Government entities and their employees, consultants, contractors and visitors are required to be aware of the consequences of not following the guidelines set by Information Security Regulation.

Dubai Government Entities that fail to comply with the guidelines found in the Information Security Regulation run the risk of exposing classified information to non-authorized parties, provide incorrect information to clients, or prevent access to critical information.

Entities/Personnel found guilty of not abiding by these guidelines may have their access to information systems revoked and may be subject to disciplinary actions in accordance to the existing laws and policies of the United Arab Emirates and the Government of Dubai.

Compliance to existing laws, or any other legislations in the future pertaining to Information Security, will take precedence over Information Security Regulation.

7 INFORMATION SECURITY REGULATION APPLICABILITY AND EXEMPTIONS

Dubai Government Entities must conduct an applicability review of the Information Security Regulation domains and controls to determine which of these domains and controls are applicable to them. Dubai Government entities must commit resources to achieve the “right-fit” implementation, while considering the risk assessment results, and keeping the controls implementation cost lower than the anticipated risk or value of information, which is being protected.

If an exemption to any portion of the regulation is required, a formal written request to DESC is to be submitted by an authorized individual from higher management within the requesting Dubai Government Entity. The request must include the description and justification of the exemption.

DESC will review the exemption requests, and will make its final decision based on the review of the written request.

8 INFORMATION SECURITY REGULATION STRUCTURE

The information Security Regulation is broken down into thirteen domains. Each domain takes into consideration one or more major classes of information security: Governance, Operation, and Assurance.

The Governance domains set high-level requirements for structuring and managing information security. The Operation domains are technical and/or non-technical controls an entity may use depending on the results of their risk assessment study. The Assurance domains act as the quality assurance for the entity, ensuring that the implemented solution is working as intended.

TABLE 1. INFORMATION SECURITY REGULATION DOMAINS AND CLASSES

DOMAINS	CLASSES		
	GOVERNANCE	OPERATION	ASSURANCE
Domain 1 – Information Security Management and Governance	✓		
Domain 2 – Information and Information Asset Management	✓	✓	
Domain 3 – Information Security Risk Management	✓	✓	
Domain 4 – Incident and Problem Management		✓	
Domain 5 – Access Control		✓	
Domain 6 – Operations, Systems and Communication Management		✓	
Domain 7 – Business Continuity Planning	✓	✓	
Domain 8 – Information Systems Acquisition, Development and Management		✓	
Domain 9 – Environmental and Physical Security		✓	
Domain 10 – Roles and Responsibilities of Human Resources	✓	✓	
Domain 11 – Compliance and Audit	✓		✓
Domain 12 – Information Security Assurance and Performance Assessment	✓		✓
Domain 13 – Cloud Security	✓		✓

The Information Security Regulation has been structured as follows:

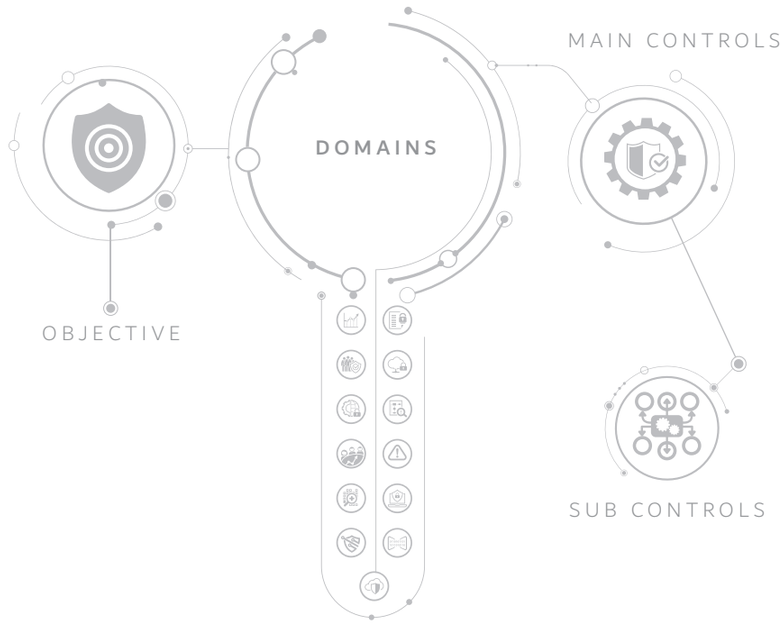
A. Domains: Reflect a key process within information security

B. Objective: Reflects what is to be achieved from the domain

C. Controls: Reflect what is to be applied to achieve the objective

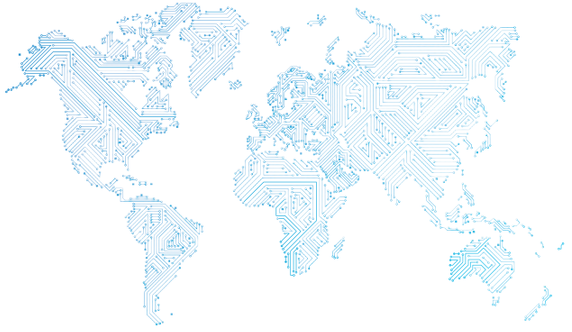
D. Sub Controls: Reflect subordinate detailed controls to the main control

INFORMATION SECURITY REGULATION STRUCTURE



INFORMATION SECURITY
REGULATION

DOMAIN 1
Information Security Management and Governance



OBJECTIVE:

To emphasize the importance of having information security as part of the overall enterprise governance through providing the following:

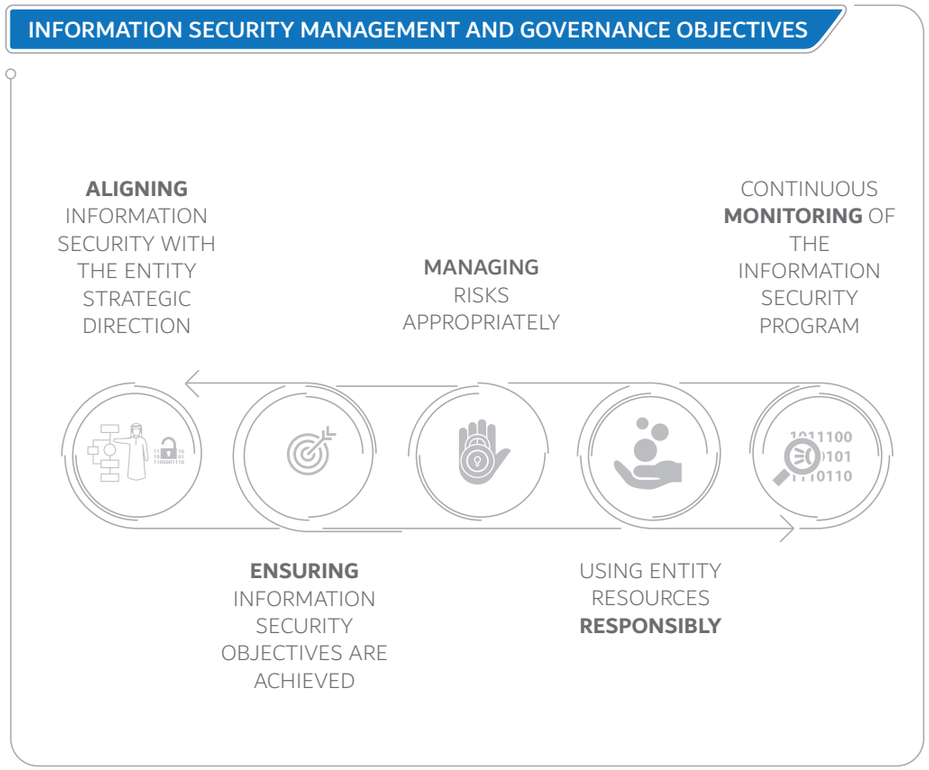
A. Aligning Information security with the entity strategic direction

B. Ensuring information security objectives are achieved

C. Managing risks appropriately

D. Using entity resources responsibly

E. Continuous monitoring of the information security program



Main Control - 1.1 Roles and Responsibilities of Information Security:

The main goals of determining the roles and responsibilities of information security are to clarify the roles of individuals, identify accountability, maintain segregation of duties, and to omit any conflict of interests. Therefore, to develop a complete information security strategy, policy and corresponding program in the entity, all roles and responsibilities in relation to information security should be clearly set and defined as tentatively and generically suggested below or in any other entity-specified approach that doesn't conflict with the requirements of this control:

Sub Control - 1.1.1 Board of Directors:

1.1.1.1 The board of directors should accept the responsibility of information security and present commitment towards it.

1.1.1.2 The entity's board of directors is assigned the responsibility of overseeing a properly managed and implemented information security program/management system and reviewing risk assessment reports.

Sub Control - 1.1.2 Director General / CEO:

1.1.2.1 The CEO or Director General who might be reporting to the board of directors has responsibility for:

A. Accepting and endorsing the overall responsibility of information security

B. Enforcing organization wide information security management system

C. Enforcing information security policies implementation across the entity

D. Overseeing and monitoring division's compliance to information security management system and information security policies.

E. Enforcing accountability towards information security

Sub Control - 1.1.3 Information Security Steering Committee:

1.1.3.1 An information security steering committee, headed by Director General or deputy, should be established and should include heads from each division in the entity. The steering committee should maintain the following roles and responsibilities:

A. Supervise and ensure the implementation of an Information Security Management System and its controls across the Entity.

B. Conduct periodical reviews on the implementation of Information Security Regulation and any information security controls and objectives.

C. Review and approve periodically the information security policies and procedures for implementation within the entity.

D. Promote Information Security culture within Entity.

E. Ensure that relevant information security methodologies are part of all business processes and any new initiatives or projects across all the entity departments or functions.

F. Follow up and review both internal and external audits results for effectiveness of Information Security Regulation implementation and ensure necessary and timely corrective actions are taken.

G. Review and approve the information security risk assessment methodology and risk assessment related results that is used across the entity.

H. Ensure that adequate resources are provided to implement, support and operate the information security management system.

I. Make recommendations for both corrective and preventive actions based on the risk assessment approach.

J. Review the Information Security Incidents and their responses.

K. Ensure that recommendations approved by the committee are implemented.

L. Ensure that Information Security requirements are integrated as part of contractual requirements in their respective project management activities.

Sub Control - 1.1.4 Senior Management:

1.1.4.1 The entity's senior management is assigned the following responsibilities:

A. Ensure that each employee understands his/her information security-related responsibilities after reading the information security policy and acknowledges through a formal sign-off that he/she understands and intends to comply with those requirements.

B. Determine the criticality and business risk of their information systems and information assets.

C. Periodically assess information assets and their associated risks.

D. Communicate the risk assessment results to relevant stakeholders.

E. Determine and review the privileges related to their information assets and information systems on a periodic basis.

F. Implement information security policies and procedures to cost-effectively reduce risk to acceptable levels.

G. Periodically, ensure conducting technical security testing on the information systems.

H. Ensure reporting of any evidence of information security compromise or any suspicious activity that could potentially expose, corrupt or destroy entity's information.

I. Respond to information security incidents.

J. Ensure that information security requirements are incorporated on respective department's project activities/contracts.

Sub Control - 1.1.5 Information Security position:

1.1.5.1 Dubai Government Entity allocates the responsibility of information security to a capable and independent position, reporting to the Top Management or to the Steering Committee, while considering the segregation of duties and omitting the conflict of interests. Hence, the information security position is assigned the following responsibilities:

A. Plan, implement and maintain an information security program/ management system that is integrated with the whole entity's processes.

B. Coordinate with the senior management on the identification, development, secure handling and management of entity wide information assets.

C. Plan, develop and maintain an organization wide information security risk assessment methodology in coordination with the higher management in the entity.

D. Ensure that appropriate operational controls are selected and implemented according to the results of the risk assessment.

E. Develop the required policies, and procedures, based on results of the risk assessment.

F. Ensure organization wide compliance to the information security program/management system and report ISR implementation status to the information security steering committee.

G. Assist and support senior management with their information security responsibilities.

H. Plan and conduct periodic information security awareness, education and training for entity's staff and applicable external parties.

Sub Control - 1.1.6 Employees:

1.1.6.1 Senior management assigns the coordination of information security activities to certain employees acting as Information security champions/ representatives/coordinators across all divisions.

1.1.6.2 The entity assigns all employees responsible for adhering to the information security policies/processes/program and for reporting any security breaches or incidents to their direct management.

Main Control - 1.2 Information Security Policy:

Sub Control - 1.2.1 Information Security Policy Document:

Dubai Government Entity

1.2.1.1 Develops, distributes and maintains an entity-wide information security policy outlining the basic principles of protecting all the information assets of the entity, and make all employees within the entity and relevant external parties aware of the potential security threats and associated business risks.

1.2.1.2 Ensure the Information security policy is approved by top management, published and communicated to employees and relevant external parties

Sub Control - 1.2.2 Information Security Policy Alignment with the Entity Strategy:

Dubai Government Entity

1.2.2.1 Aligns the information security policy with the entity overall strategy to facilitate the implementation of the entity's goals and objectives, and to support its business model without setting any obstacles in implementing them.

Sub Control - 1.2.3 Review of Information Security Policy:

Dubai Government Entity

1.2.3.1 Sets a clear responsibility for a regular review of the information security policy to be conducted at least once a year, and/or along with any changes that the entity might undergo.

1.2.3.2 Reports any update or review of the information security policy to the Information Security Steering Committee and sets the declaration of changes to the entity's CEO/Director General.

Main Control - 1.3 Technical and Operational Policies:

Dubai Government Entity

1.3.1 Develops, distributes and maintains a set of technical/operational information security policies that covers the required security protection measures and controls based on the results of the risk assessment and depicts the overall responsibility of all stakeholders in safeguarding the respective business process related information assets.

1.3.2 Supplements the entity's technical/operational policies, as necessary, with a set of procedures and guidelines that cover the implementation details of the policies in accordance with the risk assessment results.

Main Control - 1.4 Information Security Awareness and Training:

Dubai Government Entity

1.4.1 Designs, develops, and implements an information security awareness program throughout the year (that is categorized based on job roles, divisions or as the entity specifies) which is composed of targeted information security awareness creation activities in line with entity's information security related policies.

1.4.2 Provides basic information security training and awareness to all personnel within the entity, to be delivered by skilled / competent resources, as part of initial training for new users, when required by information systems changes, and in an entity specified periodic intakes.

1.4.3 Provides periodic and adequate information security trainings, to be delivered by skilled / competent resources for the employees taking part in operating the information security program/management system within their respective business areas.

1.4.4 Designs and maintains the information security awareness materials that educates users on information security policies and covers entity's business operations' security risk and focus on reducing possible business risks.

1.4.5 Conduct periodic security awareness surveys to measure the security training effectiveness and the awareness level of all entity's personnel and applicable external parties, in order to point out common mistakes or misunderstandings in information security concepts, and to improve the overall awareness program.

1.4.6 Documents information security training and awareness attendance records for all personnel.

Main Control - 1.5 Confidentiality Agreements:

Dubai Government Entity

1.5.1 Develops, and regularly reviews a non-disclosure or confidentiality agreement which is signed by all employees and external parties, that addresses in legally enforceable terms, the need for protecting the Government information from being leaked internally or externally, and emphasizing the «need to know» concept.

1.5.1 Educates personnel and makes them aware of the confidentiality of government information and how information leakage, written or spoken, can impact the entity.

Main Control - 1.6 Relations and Sustainability of Information Security:

Dubai Government Entity

1.6.1 Maintains appropriate contacts with relevant authorities within the field of information security;

1.6.2 Identifies key contacts of certain security and judicial authorities to be contacted in the cases of information security incidents, breaches, etc.

1.6.3 Maintains interactions and/or memberships with information security interest groups, forums and associations, in order to keep up-to-date information in the field of information security.

Main Control - 1.7 Securing External Parties' Relations:

Dubai Government Entity

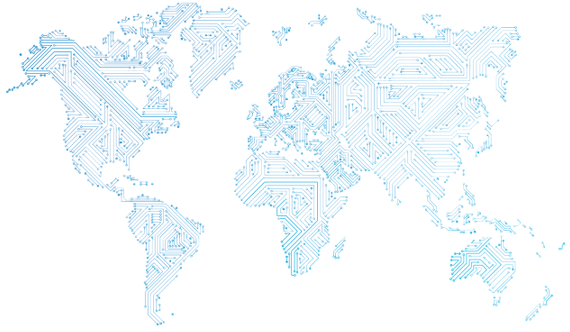
1.7.1 Determines and assesses governance and information security risks related to its relations with external parties, such as customers, external party services providers, business consultants, temporary employments, etc. This also includes outsourcing and cloud services providers.

1.7.2 Selects and applies the appropriate information security controls and measures to control the identified risks.

1.7.3 Develops and implements the required agreements to secure relations with the external parties, including integrity, availability and confidentiality.

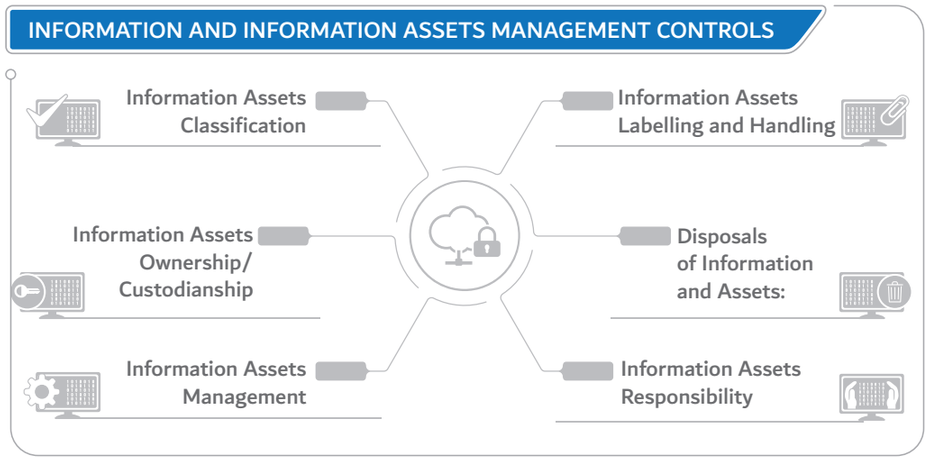
INFORMATION SECURITY
REGULATION

DOMAIN 2
Information and Information Assets Management



OBJECTIVE:

To identify and classify the information assets, and define the proper storage and handling & secure disposal measures in order to protect the entity from legal liabilities, losses, attacks, etc.



Main Control - 2.1 Information Assets Management:

Dubai Government Entity

2.1.1 Develops, distributes and maintains an entity wide information asset management policy and procedure or framework for the identification, management and protection of information assets in line with applicable laws and regulations.

2.1.2 Identifies, documents, and maintains a register of all critical information assets for the entire entity, including the information and data assets and the related information processing facilities and components, such as software assets, people assets, physical assets, etc. and consider other details such as, information classification, physical location, license details, business value, and any other necessary information that may be required to avoid risks and recover from disasters.

2.1.3 Reviews & maintains the information asset register on a regular basis.

Main Control - 2.2 Information Assets Ownership/Custodianship:

Dubai Government Entity

2.2.1 Establishes and implements information ownership policy, where information assets are identified with an owner and a custodian. Business processes, services, applications, information systems, or set of data are examples of assets that ownership and custodianship should be allocated to.

2.2.2 Assigns the information assets owner the responsibility of ensuring that proper classifications of information are carried out based on the sensitivity of information.

2.2.3 Assigns the information assets owner the responsibility of defining the proper access control to the information and ensuring periodic review of access in accordance with assigned classification level and the entity's access control policy.

2.2.4 Assigns the custodians the responsibility of maintaining the day to day operational tasks related to the information assets, while considering the higher authority of the assets by the owners.

Main Control - 2.3 Information Assets Classification:

Dubai Government Entity

2.3.1 Defines and implements an information classification scheme/ process to be used within the entity based on information assets criticality, value, legal and protection requirements, etc. in line with applicable laws and regulations (ISR Ref. 11.1 and 11.2).

2.3.2 Develops, distributes and maintains information classification policy and related procedures in line with applicable laws and regulations (ISR Ref. 11.1 and 11.2).

Main Control - 2.4 Information Assets Labelling and Handling:

Dubai Government Entity

2.4.1 Defines and implements adequate labelling and handling controls for the information assets (electronic and physical); according to the requirements of each classification level, considering the handling requirements, storage procedures, distribution limitations, etc., for each information asset.

2.4.2 Develops, distributes and maintains procedure for the information assets labelling and handling requirements

Main Control - 2.5 Disposals of Information and Assets:

Dubai Government Entity

2.5.1 Identifies and implements the required safety and security measures prior to the disposal of information or information assets based on their value, criticality and sensitivity.

2.5.2 Develops, distributes and maintains clear procedure for the process of disposal of information and information assets, as part of the labelling & handling procedure.

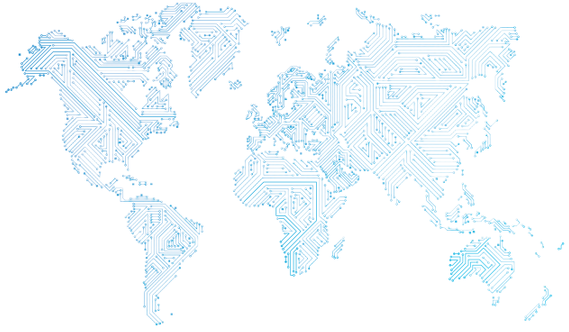
Main Control - 2.6 Information Assets Responsibility:

Dubai Government Entity

2.6.1 Develops, distributes and maintains an acceptable use policy governing the acceptable use of information and assets including usage of personal devices in entity's environment.

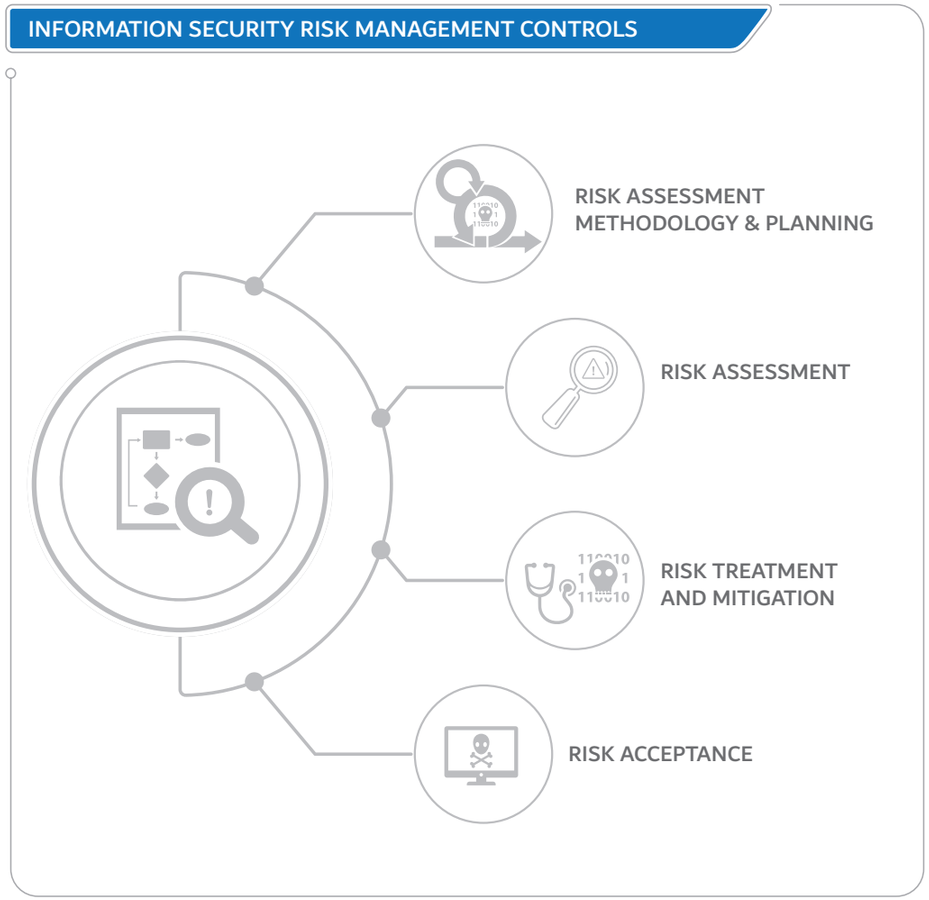
INFORMATION SECURITY
REGULATION

DOMAIN 3
Information Security
Risk Management



OBJECTIVE:

To identify and treat risks associated with critical information and information assets through a detailed study of business processes, in determining threats and vulnerabilities and accordingly apply the appropriate risk treatment plans and controls.



Main Control - 3.1 Risk Assessment Methodology & Planning:

Dubai Government Entity

3.1.1 Develops a risk assessment methodology that aligns with the requirements of the entity's information security program/management system.

3.1.2 Determines a periodic plan for conducting the risk assessment across the entity.

3.1.3 Identifies the criteria of acceptable risks as part of the risk assessment methodology.

3.1.4 Identifies the scope of the risk assessments involving key stakeholders, around their business processes & respective information assets that will be included in the assessment.

3.1.5 Identifies threats and vulnerabilities in line with risk assessment methodology.

3.1.6 Plans and implements a periodic awareness of the risk assessment program across the entity.

Main Control - 3.2 Risk Assessment:

Dubai Government Entity

3.2.1 Conducts & maintains a detailed risk assessment in accordance with the approved risk assessment methodology.

3.2.2 Analyses risks and prioritizes them based on the criticality, in order to set treatment plans and controls.

3.2.3 Determines and identifies the acceptable risks in accordance with the risk assessment methodology.

3.2.4 Documents the risk assessment results and approves it officially by the Information Security Steering Committee or higher management.

Main Control - 3.3 Risk Treatment and Mitigation:

Dubai Government Entity

3.3.1 Selects the proper risk treatment plans (mitigate, avoid, transfer, etc.) for the identified risks.

3.3.2 Determines and selects the appropriate security operational controls (under operational domains within this document) for mitigating the identified risks.

3.3.3 Signs off and authorizes officially the implementation of the risk mitigations controls.

3.3.4 Performs and implements the mitigation controls for the risks identified.

3.3.5 Reviews and monitors the implemented risk mitigation controls for effectiveness.

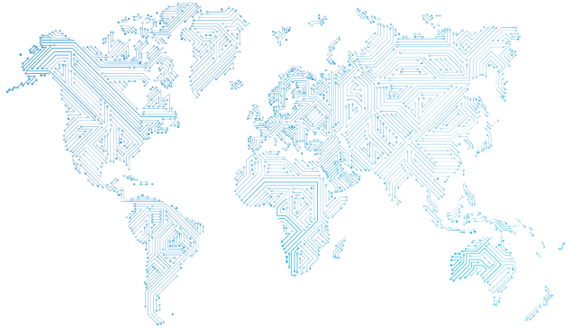
Main Control - 3.4 Risk Acceptance:

Dubai Government Entity

3.4.1 Documents the residual non treated risks with justifications and gets it signed off from the Information Security Steering Committee along with the detailed plan for treatment at a later date.

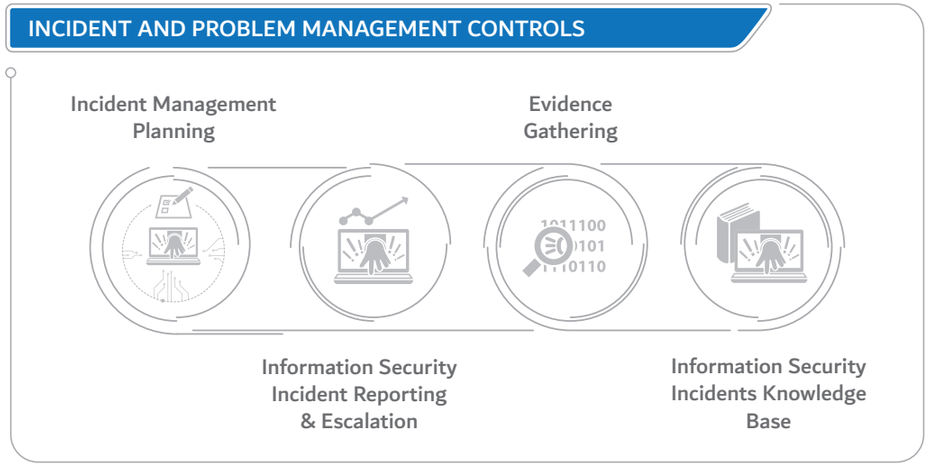
INFORMATION SECURITY
REGULATION

DOMAIN 4
Incident and Problem Management



OBJECTIVE:

To outline a proper process for the identification and effective handling of information security incidents in order to minimize the adverse impact on the business of the entity.



Main Control - 4.1 Incident Management Planning:

Dubai Government Entity

4.1.1 Develops, distributes and maintains a formal policy and procedure for the management of information security incidents.

4.1.2 Establishes a capability (Incident Response Team) for the information security incidents response and handling across the entity.

4.1.3 Provides periodic awareness and training sessions to Incident Response Team on incident handling process in order to exercise & execute effective handling of information security incidents.

Main Control - 4.2 Information Security Incident Reporting & Escalation:

Dubai Government Entity

4.2.1 Assigns responsibility to all employees or any users dealing with the entity's information, through any means, for reporting promptly any observed or suspected information security incidents or weaknesses in systems or services, to the responsible entity's team.

4.2.2 Implements an escalation process for reporting information security incidents identified as high severity for the entity and identifies and engages external authorities for further investigation if needed for such incidents.

Main Control - 4.3 Evidence Gathering:

Dubai Government Entity

4.3.1 Implement a process to gather and retain evidences related to any information security incidents.

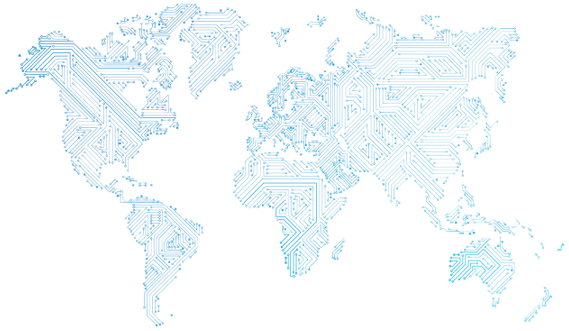
Main Control - 4.4 Information Security Incidents Knowledge Base:

Dubai Government Entity

4.4.1 Develops a knowledge base from all information security incidents which includes details of previous incidents, their types, cost, and any other relevant information.

INFORMATION SECURITY
REGULATION

DOMAIN 5
Access Control



OBJECTIVE:

To secure and protect the logical and physical access to entity's information, information processing facilities, and resources.

Main Control - 5.1 Access Control Management Policy/Procedure:

Dubai Government Entity

5.1.1 Develops, distributes and maintains an access control policy that addresses all security requirements for the implementation of an effective access control within the entity.

5.1.2 Develops, distributes and maintains an access control procedure that provides implementation details for access control, based on role-bases access control.

5.1.3 Maintains a secure repository of all information systems access controls.

Main Control - 5.2 Logical Access Control:

Sub control - 5.2.1 Users Access Control:

Dubai Government Entity

5.2.1.1 Defines and implements a process for users registration, de-registration, and users access privileges modification, disabling or removal, etc.

5.2.1.2 Provides each user with a unique identifier (user ID) for their individual business use only.

5.2.1.3 Implements a unified users ID standard across the entity.

5.2.1.4 Implements a proper authentication technique for the validation of claimed identities of users regarding access being onsite and remote.

5.2.1.5 Develops, distributes and maintains appropriate authentication policy (ies) (e.g. a password management policy that clearly addresses the password allocation process, users' responsibilities on passwords use and the recommended password structure, etc.).

5.2.1.6 Identifies the categories of users requiring regular and special privileges by ensuring the availability of the following:

A. A valid and approved access authorization.

B. Intended system usage.

C. Other attributes as required by the entity or associated missions/ business functions.

D. Utilization of access accounts with special privileges must be restricted for their intended purpose.

5.2.1.7 Maintains records of all users' access privileges, and monitors them on a continuous basis.

5.2.1.8 Limits the number of special/high privileged user IDs to those individuals who absolutely must have such privileges for authorized business purposes.

5.2.1.9 Implements proper security and independent monitoring controls over the usage of special or high privileged IDs.

5.2.1.10 Implements proper process for guest and temporary user IDs request and employs automated user IDs termination.

5.2.1.11 Allocates access privileges on a restricted basis while employing least privilege concept and separation of duties.

5.2.1.12 Employs a process for review and re-authorization of user access rights on a periodic basis, as defined by the entity.

Sub control - 5.2.2 Network Access Control:

Dubai Government Entity

5.2.2.1 Develops, distributes and maintains a policy for network access control, which covers details about accessible networks and networks services, authorization process for granting network access, etc.

5.2.2.2 Defines a process for authorizing, activating and terminating any network connections in the entity.

5.2.2.3 Implements a proper network access control tool/method for network equipment/devices connectivity detection, identification and authentication.

5.2.2.4 Implements proper authentication tool for remote access connections.

5.2.2.5 Manages and controls access to configuration ports on network equipment / devices.

5.2.2.6 Implements proper segregation controls on the different types of networks (internal, external, wireless, IP telephony, etc.)

5.2.2.7 Implements proper security and operational controls for any network connections beyond the entity's direct control.

Sub Control - 5.2.3 Operating System Access Control:

Dubai Government Entity

5.2.3.1 Manages and controls access to operating systems through secure log-on process.

5.2.3.2 Assigns each user with a unique user ID and apply the proper authentication method for identity verification.

5.2.3.3 Limits the use of generic user IDs to only exceptional and business justified circumstances, and implements the proper accountability technique for such use.

5.2.3.4 Implements an entity wide authentication mechanism to enforce various authentication controls.

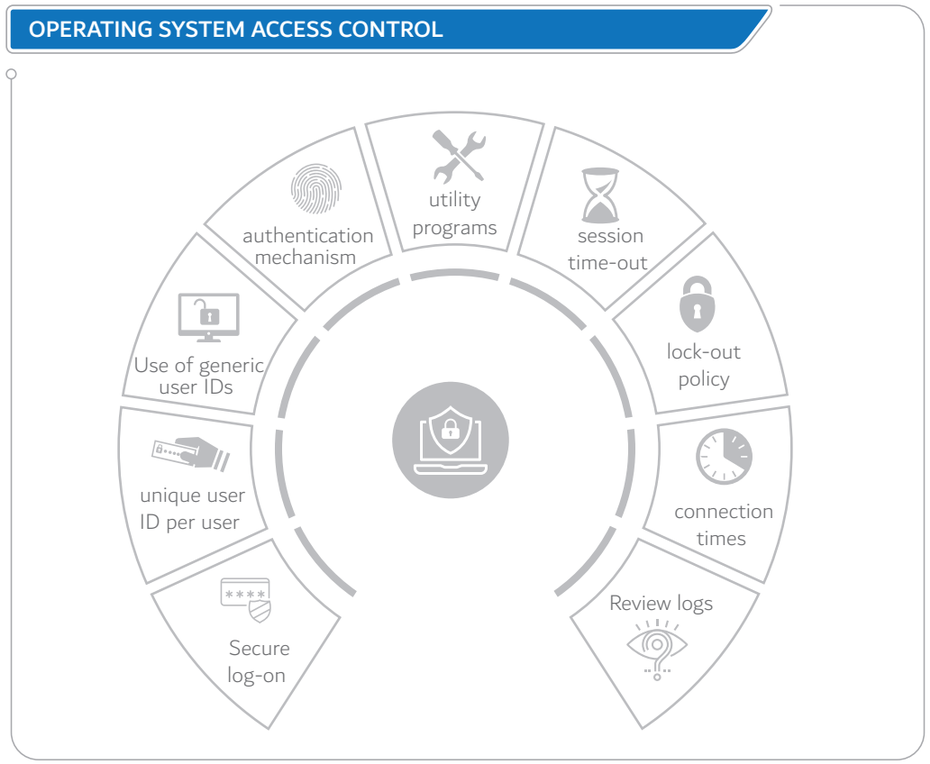
5.2.3.5 Manages and controls the use of utility programs.

5.2.3.6 Implements session time-out controls to prevent unauthorized access.

5.2.3.7 Implements lock-out policy.

5.2.3.8 Restricts connection times for critical information systems and applications.

5.2.3.9 Records and continuously reviews logs of administrators system IDs.



Sub control - 5.2.4 Applications Access Control:

Dubai Government Entity

5.2.4.1 Provides access to applications based on job responsibilities and business justifications, in alignment with the entity access control policy/ procedure.

5.2.4.2 Implements proper physical or logical isolation controls for highly critical information systems and application environments.

Sub Control - 5.2.5 Remote Access Security:

Dubai Government Entity

5.2.5.1 Develops, distributes and maintains a policy addressing remote access to the entity's resources.

5.2.5.2 Enforces formal authorization prior to remote access connections.

5.2.5.3 Ensures that adequate security controls are implemented on the VPN client machines, such as authentication, encryption, antivirus software, personal firewalls, session timeout, content filtering etc.

5.2.5.4 Provides remote access users with access to the services, which the users are specifically authorized to use.

5.2.5.5 Monitors and periodically reviews the remote access connections logs.

Sub Control - 5.2.6 Mobile Computing:

Dubai Government Entity

5.2.6.1 Develops, distributes and maintains a formal policy governing the appropriate use of mobile computing and communication facilities.

5.2.6.2 Implements appropriate security controls to protect against the risks of mobile computing and communication facilities' usage, such as:

A. Implement encryption mechanisms to protect sensitive information

B. Ensure secure handling for the portable computing devices.

C. Implement proper mechanisms to disable portable computing devices or wipe device data when lost or stolen.

D. Proper data backup procedures for the portable computing devices.

E. Limit or restrict usage of portable computing devices to authorized users with adequate security controls.

5.2.6.3 Develops, distributes and maintains a policy and procedure for the handling and usage of personally owned devices (Bring your own Device (BYOD)) that are not owned by the entity, addressing entity's security requirements on handling lost or stolen portable computing devices, storage of entity data on these devices, connectivity to entity network and systems etc.

Sub Control - 5.2.7 Wireless Access Management:

Dubai Government Entity

5.2.7.1 Develops, distributes and maintains a formal policy on the wireless network usage.

5.2.7.2 Authorizes formally the wireless access to the network prior to any connection.

5.2.7.3 Implements the proper authentication controls for the wireless access.

5.2.7.4 Enforces proper security controls for wireless connections to the entity's network and establishes usage restrictions and implementation guidance for such use.

5.2.7.5 Provides wireless connection users with access to services that they have been specifically authorized to use.

5.2.7.6 Monitors continuously the unauthorized wireless access to the network.

Main Control - 5.3 Physical Access Control:

Sub Control - 5.3.1 Physical Access Policy and Procedure:

5.3.1.1 Develops, distributes and maintains a formal documented physical access policy that addresses the entity's requirements for implementing physical access controls on offices, rooms and other areas.

5.3.1.2 Supplements, as necessary, the physical access policy with a detailed procedure on how to implement the protection controls and provides users with complete specification on physical security safeguards.

5.3.1.3 Enforces formal authorization prior to physical access to any facilities with information processing resources.

Sub Control - 5.3.2 Physical Security Controls:

Dubai Government Entity

5.3.2.1 Enforces appropriate physical access control perimeters for all physical access points to the entity.

5.3.2.2 Verifies and ensures that only authorized employees are provided access to protected areas.

5.3.2.3 Controls entry to the data center, or any facility containing information systems using physical access control devices.

5.3.2.4 Controls and monitors physical access to the information processing facilities areas or any other public areas.

5.3.2.5 Safeguards and enforces adequate protection controls on physical access devices.

5.3.2.6 Keeps inventory of all physical access devices owned by the entity.

5.3.2.7 Reviews logs of physical access on a regular basis.

5.3.2.8 Deploys mechanism to monitor the movement of employees & non-employees within the entity.

Main Control - 5.4 Public and External Party Access Control:

Dubai Government Entity

5.4.1 Enforces formal authorization prior to logical or physical access required by external party through deploying a «need to know» criteria

5.4.2 Monitors and logs logical or physical access provided to public or external party.

5.4.3 Controls physical access to any areas that includes information systems and other areas such as delivery, loading, or any other points where unauthorized personnel may enter by authenticating visitors before authorizing access.

5.4.4 Authorizes, monitors, and controls entering and exiting the data centre facilities or any other public areas and maintains such records.

5.4.5 Sets physical access protection and control mechanisms on all external parties or outsourced individuals and hold them liable for any violation or compromising the entity's information security policy.

Main control - 5.5 Information and Documents Access Control:

Dubai Government Entity

5.5.1 Places adequate security controls on accessing and handling all soft / hard documents / information in alignment with its criticality.

5.5.2 Determines and assigns the needed access rights for the protected documents/information.

5.5.3 Sets a clear policy on controlling documents, along with defining a clear retention period for archiving, and supplementing it with procedures and guidelines for implementation and usage.

5.5.4 Employs a procedure for the disposal of documents, with requirements of authorization and responsibilities.

Main Control - 5.6 Access Control Audit and Review:

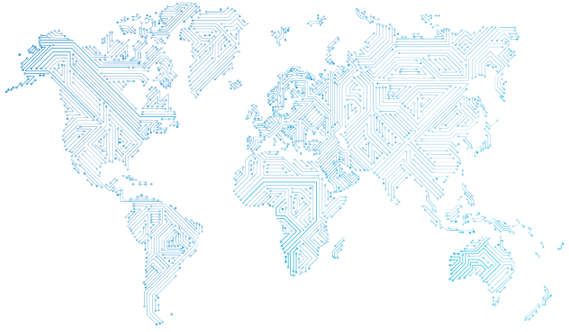
Dubai Government Entity

5.6.1 Implements audit trails in information processing systems, as necessary.

5.6.2 Logs, maintains and periodically reviews logical and physical access control lists.

INFORMATION SECURITY
REGULATION

DOMAIN 6
Operation, Systems and Communication Management



OBJECTIVE:

To set controls for mitigating the risks associated with the daily operations of information processing systems, applications, network and communication tools being used internally and/or with external party.

Main Control - 6.1 Operations Management:

Sub Control - 6.1.1 Technology and operations Capacity Management:

Dubai Government Entity

6.1.1.1 Ensures advanced planning and preparation for availability of adequate capacity and resources for the information processing systems and their technology components, and in line with applicable regulations.

6.1.1.2 Conducts an annual projection review of capacity requirements and resources for the information processing systems and their technology components, integrating business requirements.

Sub Control - 6.1.2 Documentation of Operational Procedures:

Dubai Government Entity

6.1.2.1 Develops and maintains a complete set of operating procedures documentations of all information processing systems detailing inputs, outputs and dependencies.

6.1.2.2 Documents and maintains up to date baseline configurations manuals of all information processing systems including an inventory of constituent system components.

6.1.2.3 Places adequate security protection controls on the documentation of operational procedures of all critical information processing systems, through defining a clear distribution list and permitted users and ensures their availability to authorized users whenever required.

Sub control - 6.1.3 Change Management:

Dubai Government Entity

6.1.3.1 Develops, distributes and maintains a formal documented change management policy that defines the overall change management process employed by the entity, outlining roles and responsibilities of different business owners.

6.1.3.2 Supplements, as necessary, the change management policy with a detailed procedure to facilitate the implementation of the change and configuration management process and provide guidelines for all users.

6.1.3.3 Implements a change management process that must include the following details, as a minimum:

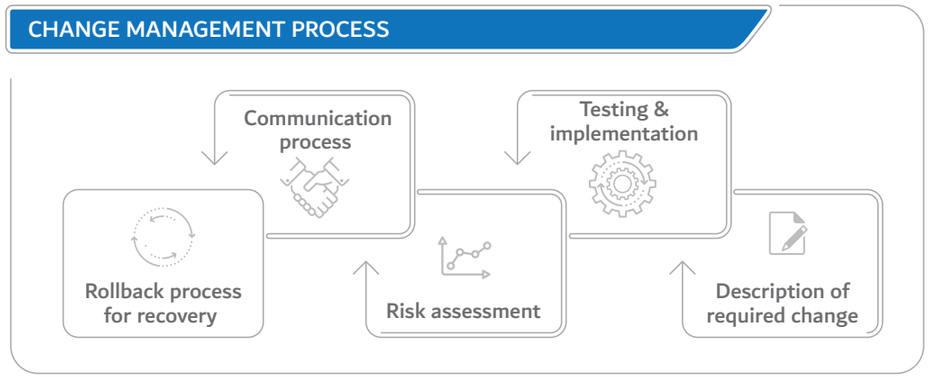
A. Description of required change.

B. Testing and implementation plans for the change.

C. Risk assessment of the change impact.

D. Official authorization of the change and the communication process for all stakeholders.

E. Rollback process for recovery of unsuccessful changes.



Sub Control - 6.1.4 Segregation of Duties:

Dubai Government Entity

6.1.4.1 Segregates duties and responsibilities as necessary through distributing the tasks for a specific business process / area among multiple users, in a manner to reduce errors, fraud and unauthorized modification or misuse of the entity's assets.

Sub Control - 6.1.5 Separation of Operational Facilities:

Dubai Government Entity

6.1.5.1 Segregates where necessary development, testing and production processing facilities to mitigate the risk impacting the production systems from unauthorized intentional or unintentional access or change.

6.1.5.2 Allocates secured computing environment for the sensitive and critical information systems facilities.

Sub Control - 6.1.6 Information Systems Deployment:

Dubai Government Entity

6.1.6.1 Develops, distributes and maintains a formal policy and procedure for the acquisition, deployment and upgrade of information systems, addressing the entity's requirements for ensuring proper security controls implementation and in line with entity's baseline configuration requirements, prior to acceptance or deployment.

6.1.6.2 Defines and implements proper acceptance criteria for new information systems implementation and upgrades, and enforcing formal certification and accreditation process outlining security requirements.

6.1.6.3 Carries out suitable security testing of the information systems during development and prior to acceptance and deployment, and ensures periodic testing.

Sub control - 6.1.7 Virtualization Techniques:

Dubai Government Entity

6.1.7.1 Employs virtualization techniques, as necessary and whenever applicable, along with deployment of the proper security controls, which can help, when properly implemented, in reducing the likelihood of successful security attacks.

Main Control - 6.2 External Party Services Management:

Dubai Government Entity

6.2.1 Develops, and maintains a formal agreement with the external party service providers that addresses compliance with the entity information security requirements.

6.2.2 Places adequate measures to assure that security controls, services definitions and delivery levels agreed upon in the external party contractual agreements are implemented and followed by the external party.

6.2.3 Monitors, reviews and audits the services and all related deliverables provided by external party in a regular basis.

6.2.4 Places adequate measures to manage and assess risks related to changes of the external party services. Examples of changes may include:

A. Application of new or enhanced security controls.

B. Updating entity's policies/procedures.

C. New technology or new vendor to be used.

Main Control - 6.3 Protection against Malicious and Mobile Code:

Dubai Government Entity

6.3.1 Develops, distributes and maintains a formal policy covering the requirements for prevention, detection and recovery controls against malicious codes.

6.3.2 Conduct regular awareness across the entity on the importance of protecting the entity infrastructure from malicious code attacks.

6.3.3 Implements a proper entity wide system/software for the malicious code scanning, detection and repairing.

6.3.4 Keeps an up to date malicious code protection mechanisms which are continuously updated.

6.3.5 Performs periodic scans of all information systems and real time scans of files from external sources as the files are downloaded, opened, or executed, as defined by the implemented policies.

6.3.6 Automates the antivirus software configurations, updates and operations among all users and employees.

6.3.7 Establishes and maintains appropriate informative communication channels to obtain latest details of new malicious code.

6.3.8 Develops and implements proper continuity plans/procedures for recovery from malicious code attacks.

6.3.9 Defines the acceptable and unacceptable mobile code technologies.

6.3.10 Establishes formal usage restrictions and implementation guides for the acceptable mobile code technologies.

6.3.11 Enforces formal authorization, monitoring and control over the use of mobile code technologies.

Main Control - 6.4 Network Security

Dubai Government Entity

6.4.1 Implements formal process for its network services to govern the interconnections between its network, critical owned business information systems and other networks and information systems outside its formal boundaries, outlining the roles and responsibilities of securing the connections and all other requisite issues such as duration of connection, ports, users' access, etc.

6.4.2 Develops and implements network service agreements and ensures that all required security controls, service levels, and management requirements are included in such agreements.

6.4.3 Enables clock synchronization on all networking devices with agreed reference such as Universal Coordinated Time (UTC) to facilitate forensic analysis, and continuously monitor its accuracy.

6.4.4 Monitors the information system connections continuously and always verifies enforcement of security requirements.

6.4.5 Implements secure network routing controls.

6.4.6 Implements adequate protection level for the confidentiality, integrity and availability of transmitted information and, prevent unauthorized access to information or data in transit (whether within entity or to external network).

6.4.7 Terminates network connections associated with communication sessions as per the entity defined time period of inactivity.

6.4.8 Implement measures to ensure adequate/high level of network availability.

6.4.9 Configures the network traffic devices on a need basis, as the general rule of thumb is ‹deny-all› otherwise justify, with maintaining logs of all changes as per the entity's change management policy.

6.4.10 Develops and maintains full documentation of the network devices, connections, and IP configuration while ensuring highest security protection and controls on the documents.

6.4.11 Applies appropriate logging and monitoring procedures to enable recording of network security activities.

Main Control - 6.5 Information Exchange Management:

Sub Control - 6.5.1 Information Exchange:

Dubai Government Entity

6.5.1.1 Develops, distributes and maintains formal policy and procedures governing the exchange of information internally in the entity, or externally with outside entities, in all types of communication channels, based on the criticality of information and in line with relevant laws and regulations.

6.5.1.2 Develops and maintains formal information exchange agreements that cover the protection and non-disclosure requirements for the exchange of any government related information between the entity and any external party.

6.5.1.3 Applies adequate security controls on top of the process of exchanging information, specifically for transmitted physical media containing information such as labelling, liability, etc.

Main Control - 6.6 Electronic Messaging/Emails:

Dubai Government Entity

6.6.1 Develops, distributes and maintains a formal electronic communication policy that governs the use of all electronic messaging/email tools provided to the users, outlining the risks associated with it.

6.6.2 Implements mechanisms to ensure confidentiality, integrity and appropriate availability of electronic messaging/emails.

6.6.3 Deploys a process of stamping a mandatory disclaimer for electronic messaging/emails.

6.6.4 Deploys an archival and retention policy for electronic messaging/emails.

6.6.5 Deploys advanced authentication mechanisms for access to electronic messaging/emails from non-trusted networks and public networks.

6.6.6 Deploys non-repudiation supporting advanced encryption mechanisms (e.g. digital signatures) while exchanging critical and sensitive government information.

Main Control - 6.7 Online Transactions and Public Information Management:

Sub Control 6.7.1 - Online Transactions Controls:

Dubai Government Entity

6.7.1.1 Implements adequate confidentiality, integrity and availability controls over any online transactional information/services, in order to protect it from frauds, unauthorized modification or disclosure, etc.

6.7.1.2 Develops and implements the required agreements with any involved party in managing the online transactions services, and ensures the inclusion of trading terms, details of authorization, liabilities, etc.

Sub Control 6.7.2 - Public Information:

Dubai Government Entity

6.7.2.1 Protects the integrity of public information that is available on publicly accessible channels or systems such as internet websites, associated written media etc., using information security controls such as appropriate authentication and access controls, depending on the nature of the business requirements and applicable legal obligations.

6.7.2.2 Ensures compliance of information published by employees on behalf of the government entity with applicable laws, rules and regulations and approves the publication by an authorized management body within Dubai Government Entity.

Main Control - 6.8 Media Handling Management:

Dubai Government Entity

6.8.1 Implements adequate security and protection procedures for any type of media containing information, in terms of handling, storage, disposal, etc.

Main Control - 6.9 Monitoring and Logs Management:

Dubai Government Entity

6.9.1 Enables audits logs for all information processing systems/ applications, and periodically reviews such logs and ensures applying adequate retention measures over them.

6.9.2 Sets adequate monitoring requirements for all information systems/ applications based on criticality of the systems.

6.9.3 Logs system administrators and operators activities and ensures reviewing them periodically, by an independent unit.

6.9.4 Enables faults logging on all system levels including network, applications, servers and databases among others.

6.9.5 Deploys adequate logs analysis mechanism and places appropriate actions on faults.

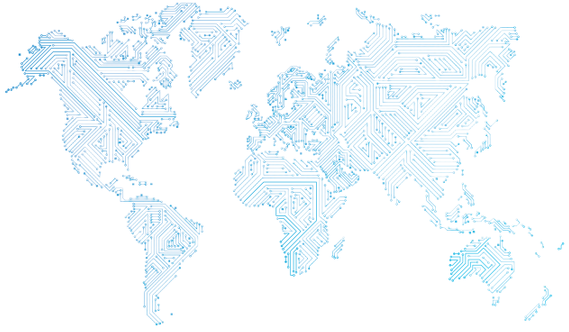
6.9.6 Secures, where appropriate, logging systems and log files against unauthorized changes including alterations, deletions, and renaming of log file contents, dates and time stamps.

6.9.7 Sets an appropriate life time for maintaining the logging information, as per the business needs and criticality of information.

6.9.8 Enables clock synchronization over all information processing systems / applications with accurate time source.

INFORMATION SECURITY
REGULATION

DOMAIN 7
Business Continuity Planning



OBJECTIVE:

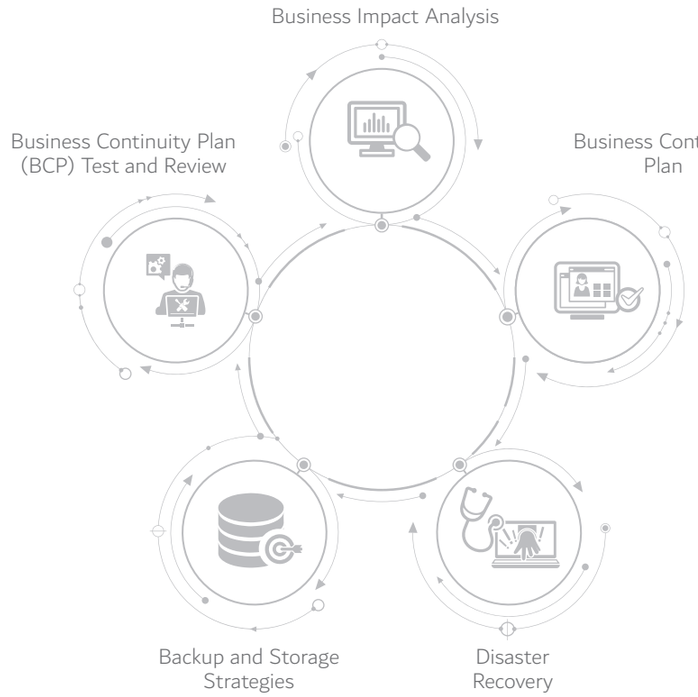
A. Ensure that critical services and business processes within the entity are available

B. Ensure that IT services are available as required

C. Ensure minimal business impact in the event of a service disruption or change

D. Ensure that IT services and infrastructure can resist and recover from failures due to errors, planned attacks or disasters

DOMAIN v BUSINESS CONTINUITY PLANNING CONTROLS



Main Control - 7.1 Business Impact Analysis:

Dubai Government Entity

7.1.1 Develops and periodically conducts a business impact analysis for all critical business processes and information systems in order to define and determine the impact of potential operational failures.

7.1.2 Sets and accounts the responsibility of the Business Impact Analysis to the senior management, with involvement from all related divisions.

Main Control - 7.2 Business Continuity Plan:

Dubai Government Entity

7.2.1 Organizes and accounts responsible a committee of senior management and business owners for the business continuity plan, with defined and clear responsibilities.

7.2.2 Develops, maintains and periodically tests and reassesses a business continuity plan that covers the following:

A. The plan should be based on the Business Impact Analysis and Risk Assessment.

B. The plan should address requirements for resilience, alternative processing and recovery capability of all critical business and IT services.

C. The plan should cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

7.2.3 Designs a business continuity process in a manner to reduce the impact of a major disruption on key business functions and processes.

Main Control - 7.3 Disaster Recovery:

Dubai Government Entity

7.3.1 Identifies the most critical business systems and applications in accordance with the risk assessment conducted by the entity.

7.3.2 Deploys a proper recovery plan for the identified critical business systems, as the entity's operations specify.

7.3.3 Determines the type of recovery scheme that is applicable for its requirement.

7.3.4 Exercises and periodically tests the decided recovery plan.

7.3.5 Implements disaster recovery sites in case their business systems result in a major loss for the whole government, through using an effective approach based on feasibility studies.

Main Control - 7.4 Backup and Storage Strategies:

Sub Control - 7.4.1 Backup and Storage Policy and Procedure:

Dubai Government Entity

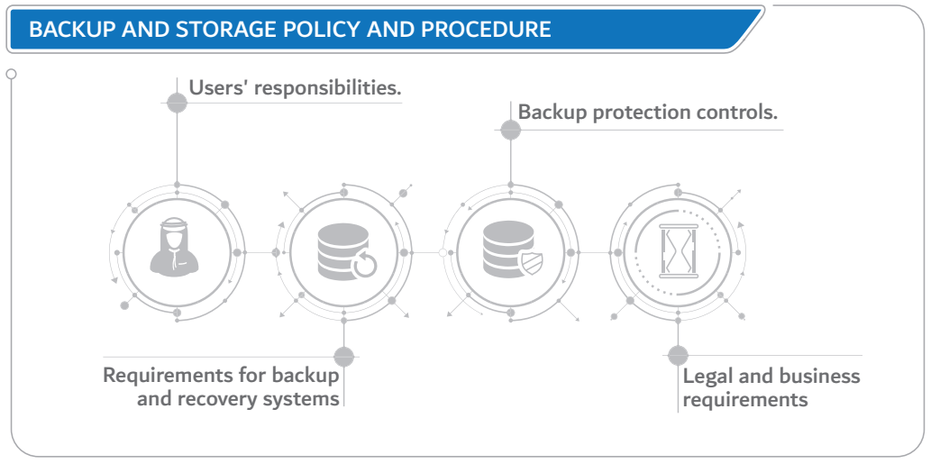
7.4.1.1 Develops, distributes and maintains a formal documented backup, storage and retention policy that includes:

A. Users' responsibilities.

B. Requirements for backup and recovery systems.

C. Backup protection controls.

D. Legal and business requirements (e.g. recovery point objective, recovery time objective, etc.).



7.4.1.2 Supplements, as necessary, the backup policy with a detailed procedure for backup and storage specifications and implements them.

Sub Control - 7.4.2 Media Library and Resources Protection:

Dubai Government Entity

7.4.2.1 Develops, distributes and maintains a formal documented policy and procedure on media library protection.

7.4.2.2 Restricts and continuously monitors access to media libraries and storage resources.

7.4.2.3 Marks clearly all media and storage resources, indicating distribution lists, handling controls, and the application asset's security classification as per the assets classification policy.

7.4.2.4 Allocates proper locations, with adequate security and environmental measures and controls for the storage of the backup media, whether onsite/ offsite, as the entity specifies.

7.4.2.5 Sets security agreements and proper security protection controls in case an external party is involved in handling the media library for the entity.

7.4.2.6 Protects and controls all physical media while being in a transit process.

7.4.2.7 Encrypts backups and archives where technically feasible and appropriate.

7.4.2.8 Maintains accountability for media in transit outside the entity control areas and restricts to authorized personnel.

7.4.2.9 Wipes and sanitizes all backup media prior to disposal or reuse.

Sub Control - 7.4.3 Backup Testing Restoration:

Dubai Government Entity

7.4.3.1 Plans and executes a periodic testing and restoration process of all backup and storage media.

Main Control - 7.5 Business Continuity Plan (BCP) Test and Review:

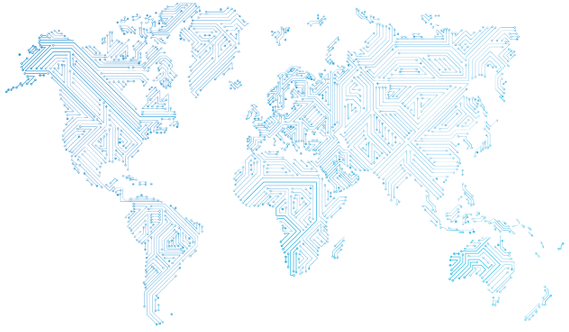
Dubai Government Entity

7.5.1 Maintains, exercises and tests in a periodic manner the Business Continuity Plan, Business Impact Analysis, Backup and Restoration, and Disaster Recovery Plan.

INFORMATION SECURITY
REGULATION

DOMAIN 8

Information Systems Acquisition, Development and Management



OBJECTIVE:

To protect information from unauthorized modification or misuse through the integration of information security into the Systems Acquisition/Development Life Cycle.

Main Control - 8.1 Information Systems Acquisition, Development and Management:

Sub Control - 8.1.1 Information Systems Acquisition, Development and Management Policy and Procedure

Dubai Government Entity

8.1.1.1 Develops, distributes and maintains a formal documented policy and procedures for addressing the entity's requirements for ensuring the security on any in house developed or external party applications regarding the Acquisition, Development and Management of information systems, including mobile applications.

Sub Control - 8.1.2 Application Development

Dubai Government Entity

8.1.2.1 Develops an Application or Software Development Life Cycle (SDLC) methodology incorporating adequate security controls at all phases of the software development life cycle, while considering the defined security requirements (e.g. functional, technical, assurance etc.) at each software development stage.

8.1.2.2 Defines, distributes and maintains a formal procedure for secure deployment, distribution, provisioning and decommissioning of portable computing device applications, application interfaces (APIs) (including third party components), through regular updates / checks to ensure adequate level of security.

Main Control - 8.2 Information Systems Security Requirements and Specifications:

Dubai Government Entity

8.2.1 Defines and documents information security requirements in all business cases, requests for proposals and work requests, related to acquisitioned or in house developed information systems, in order to ensure integrating adequate security controls and minimize any cost related to security, and sufficient resources are allocated to implement these controls.

8.2.2 Develops and approves the information systems design documents addressing the security requirements covering all the relevant platforms (e.g. operating systems, browsers, portable computing devices, etc.)

8.2.3 Develops the secure coding standards for information systems software / mobile application / web application development.

8.2.4 Designs the security architecture for the development & deployment of information systems including network security, transmission security etc.

8.2.5 Implements adequate configuration management process during information systems design, development, implementation and operation.

Main Control - 8.3 Secure and Correct Processing of Information Systems:

Dubai Government Entity

8.3.1 Conducts proper testing to validate integrity of data input controls on information systems/applications.

8.3.2 Identifies integrity requirements for processed messages and information in the information systems/applications and ensures implementing adequate controls to protect it.

8.3.3 Integrates validation checks into information systems/applications processing to detect any loss of integrity in processed information.

8.3.4 Conducts proper testing to validate integrity of data output from information systems/applications.

Main Control - 8.4 Securing Information Systems Files, Source Codes and Data:

Dubai Government Entity

8.4.1 Implements restrictive information system procedures on the installation and maintenance of software in the operational information systems environments.

8.4.2 Implements proper protection controls on the use of testing data.

8.4.3 Implements proper access control procedures on information systems/application source codes.

Main control - 8.5 Managing Changes in Software Development:

Dubai Government Entity

8.5.1 Implements proper change management controls on the software development processes, whether performed in-house or outsourced.

8.5.2 Tests and verifies the operational status of all information systems/ applications after implementing any change.

8.5.3 Implements proper controls to limit the risk of changes to software packages.

8.5.4 Implements proper controls to prevent information leakage in all information system/application environments.

8.5.5 Implements proper security controls on outsourced software/ application development covering all stages of the project including source code management, application maintenance etc.

Main control - 8.6 Security Testing:

Dubai Government Entity

8.6.1 Performs technical security reviews and vulnerability tests in order to periodically assess technical infrastructure and information systems/ applications security against latest threats and vulnerabilities.

8.6.2 Conducts periodic code reviews on all information systems/ applications developed in house or by an external party.

Main control - 8.7 Deployment of Information Systems / Applications:

Dubai Government Entity

8.7.1 Deploys the information systems/ applications into production environment after successful completion of testing & fixing of defects identified.

8.7.2 Implements security sign off process to confirm the proper implementation of security controls on all information systems/applications prior to deployment.

Main Control - 8.8 Cryptography Controls:

Dubai Government Entity

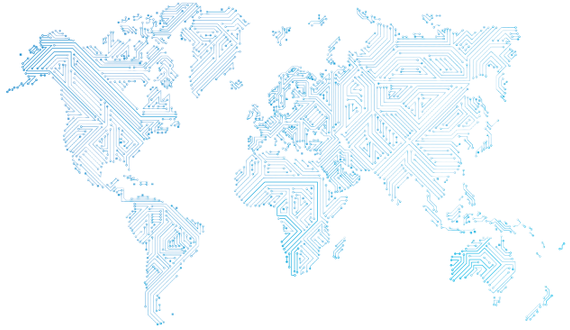
8.8.1 Develops, distributes and maintains a policy on the use of cryptography and key management wherever applicable (e.g. during development and maintenance of information systems/applications etc.).

8.8.2 Implements proper cryptography and key management mechanisms as required by the entity.

8.8.3 Implements proper protection and security controls on all cryptographic keys used by the entity.

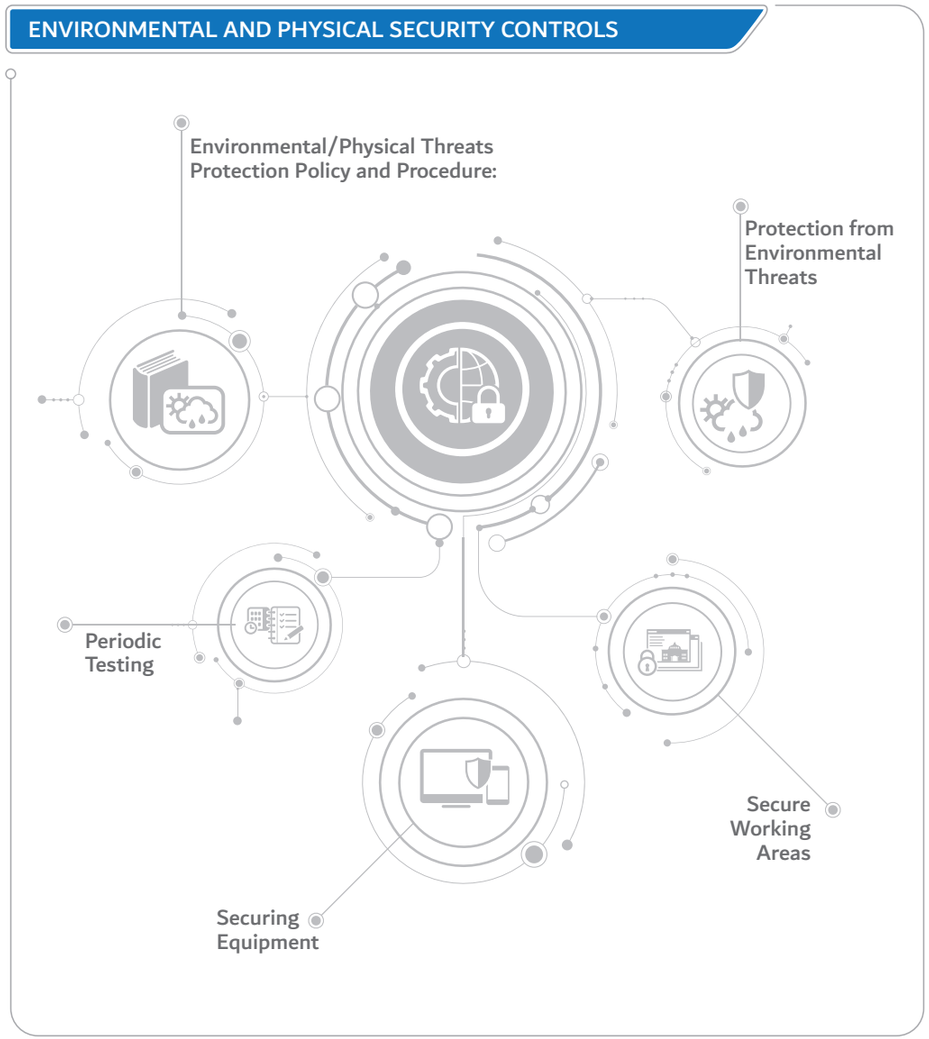
INFORMATION SECURITY
REGULATION

DOMAIN 9
Environmental and Physical Security



OBJECTIVE:

To ensure protection of the organization premises, information processing facilities and resources from physical or environmental damages.



Main Control - 9.1 Environmental/Physical Threats Protection Policy and Procedure:

Dubai Government Entity

9.1.1 Develops, distributes, and maintains a formal, documented environmental threats protection policy that addresses the entity's requirements for placing environmental protection controls.

9.1.2 Supplements the environmental threats protection policy with a formal documented procedure to facilitate the implementation of the environmental threats protection policy.

Main Control - 9.2 Protection from Environmental Threats:

Dubai Government Entity

9.2.1 Implements adequate protection controls against environmental threats, such as fire, floods, earthquakes, etc.

9.2.2 Controls humidity and temperature level on information processing facilities, and continuously monitors it.

9.2.3 Implements proper fire suppression and detection systems.

9.2.4 Implements proper control for monitoring water leakage at the physical information processing facilities.

Main control - 9.3 Secure Working Areas:

Dubai Government Entity

9.3.1 Implements adequate physical security mechanisms on offices, data centres, and other working areas, based on criticality of such areas.

9.3.2 Provides employees with proper guidelines and awareness on the implemented protection controls in the working areas.

9.3.3 Develops, distributes and maintains a clear desk and clear screen policy that addresses users' responsibilities on securing desks, working areas, and electronic user devices (e.g. PCs, printers, etc.).

9.3.4 Implements proper security controls over delivery and loading areas.

Main control - 9.4 Securing Equipment:

Dubai Government Entity

9.4.1 Places information systems related equipment in secure and protected locations.

9.4.2 Protects power equipment and cabling of information processing facilities from damages.

9.4.3 Implements UPS (uninterruptable power supply) systems to avoid power failures where deemed necessary.

9.4.4 Implements proper maintenance procedures on all information processing facilities.

9.4.5 Implements proper protection controls over equipment and information processing facilities residing offsite, including its movement, storage and handling.

9.4.6 Implements adequate security controls on the disposal or re-use of any equipment or information processing facility.

Main control - 9.5 Periodic Testing:

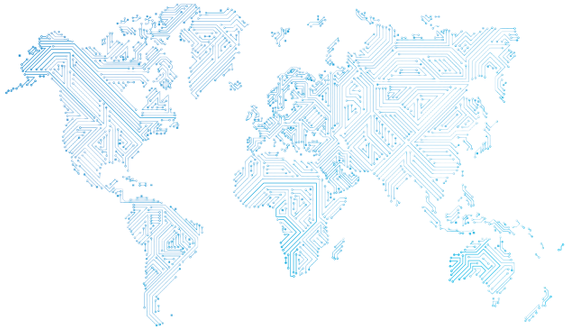
Dubai Government Entity

9.5.1 Conducts proper testing and assessment periodically over all implemented environmental and physical protection controls.

INFORMATION SECURITY
REGULATION

DOMAIN 10

Roles and Responsibilities of Human Resources



OBJECTIVE:

To ensure that all employees, contractors and outsourced employees are aware of their obligations towards information security and that their roles and responsibilities are defined in relation to securing entity's information and its processing facilities.

Main control - 10.1 Prior to Employment Security Controls:

Dubai Government Entity

10.1.1 Defines security roles and responsibilities of employees, contractors and outsourced employees in alignment with the entity high level information security policy.

10.1.2 Documents security roles and responsibilities in the job descriptions and objectives of all employees, contractors and outsourced employees.

10.1.3 Conducts proper screening and background verification for all employment candidates according to the applicable laws and policies of Dubai Government.

10.1.4 Ensures that all employment contracts define security obligations of employees, contractors and outsourced employees, and that approved candidates read and agree such obligations.

10.1.5 Incorporates Information Security Awareness as part of induction programs of newly hired employees, contractors and outsourced employees.

Main control - 10.2 During Employment Security Controls:

Dubai Government Entity

10.2.1 Accounts the senior management responsible for enforcing compliance of their employees, contractors and outsourced employees to the entity information security policies and procedures.

10.2.2 Sets a clear and defined disciplinary action for employees, contractors and outsourced employees who may breach information security policies and procedures.

10.2.3 Ensures that all employees, contractors and outsourced employees are provided with information security awareness programs on a regular basis.

Main Control - 10.3 Termination/Change of Employment Security controls:

Dubai Government Entity

10.3.1 Implements proper security controls on the process of terminating or changing employment.

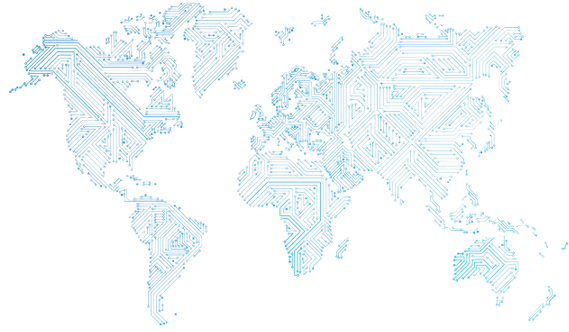
10.3.2 Communicates termination responsibilities to the terminated employee in relation to confidentiality agreements and employment contracts.

10.3.3 Implements a process for returning all entity's assets upon termination of employment.

10.3.4 Implements a process for revoking or changing access rights and privileges upon termination or change of employment.

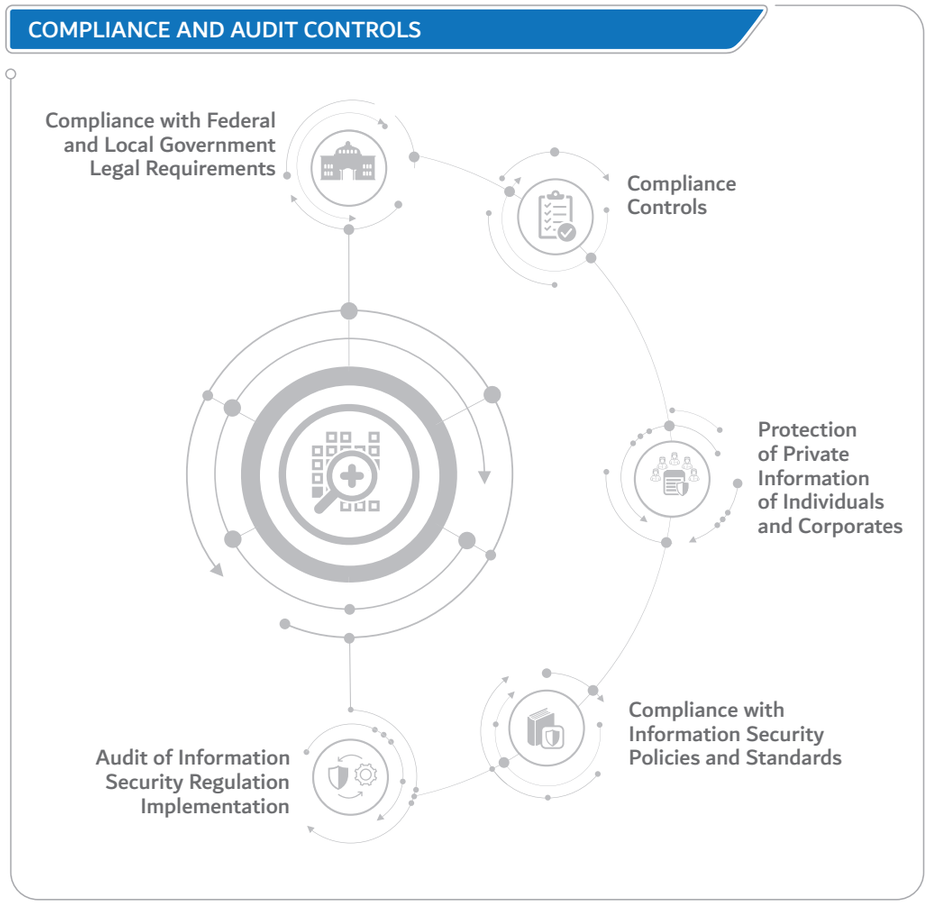
INFORMATION SECURITY
REGULATION

DOMAIN 11
Compliance and Audit



OBJECTIVE:

To clearly define compliance and audit requirements in order to ensure effectiveness of the implemented security controls and avoid any violations and breaches to any laws, policies, or controls.



Main Control - 11.1 Compliance with Federal and Local Government Legal Requirements:

Dubai Government Entity

11.1.1 Ensures compliance with the following laws and regulations:

A. Federal Law No. 1 of Year 2006 on Electronic Commerce and Transactions.

B. Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes.

C. Transactions and electronic commerce Law No. 2 issued in Year 2002 by Dubai Government.

D. The Executive Council of Dubai Government Resolution Number (13) issued in Year 2012 for Information Security Regulation.

E. The Government of Dubai Human Resources Management Law No. (27) of 2006 and its amendment

F. Dubai Electronic Security Center Law No.11 of 2014.

G. Law No.26 of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai.

H. Any other laws pertaining to information security.

Main Control - 11.2 Compliance Controls:

Dubai Government Entity

11.2.1 Identifies the laws or regulations that are applicable to the entity's scope of services.

11.2.2 Develops, distributes and maintains a formal Intellectual Property Rights (IPR) policy that defines the legal obligations pertaining to the use of information assets (e.g. hardware, software, etc.)

11.2.3 Ensures compliance with Intellectual Property Rights (e.g. software license agreements).

11.2.4 Prohibits employees from manipulating, making or distributing unauthorized copies of copyrighted/licensed materials, software or applications.

11.2.5 Implements proper protection controls for the storage, retention and disposal of entity's information assets and records.

Main Control - 11.3 Protection of Private Information of Individuals and Corporates:

Dubai Government Entity

11.3.1 Develops, distributes and maintains a privacy policy that addresses the legal requirements for the prevention of misuse of personal information of the entity's customers, for any reason.

11.3.2 Develops, distributes and maintains a formal procedure detailing the protection measures required for the processing of private data and information.

11.3.3 Conducts continuous awareness sessions on the requirements of protecting private data and information for the responsible personnel.

11.3.4 Restricts, minimizes and monitors access to personal and private data, and applies proper controls on the process of collecting, processing and transmission of personal data, which should be on «a need-to-know» basis.

11.3.5 Sets proper accountability procedures in the event of any private information and personal data leakage.

Main Control - 11.4 Compliance with Information Security Policies and Standards:

Dubai Government Entity

11.4.1 Conducts periodic reviews to verify compliance of the implemented information security policies and procedures.

11.4.2 Conducts periodic technical reviews on information systems to verify compliance with the security controls/standard

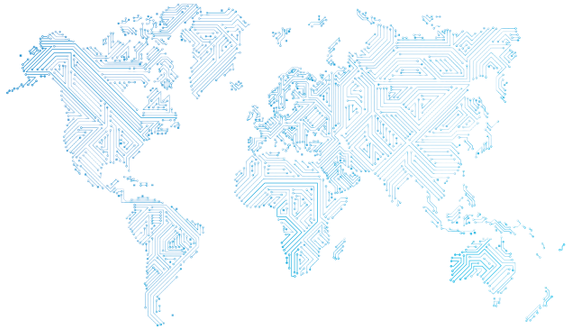
Main Control - 11.5 Audit of Information Security Regulation Implementation:

Dubai Government Entity

11.5.1 Plans and conducts internal periodic audits to verify and report effectiveness of the implementation of the Information Security Regulation.

INFORMATION SECURITY
REGULATION

DOMAIN 12
Information Security Assurance and Performance Assessment



OBJECTIVE:

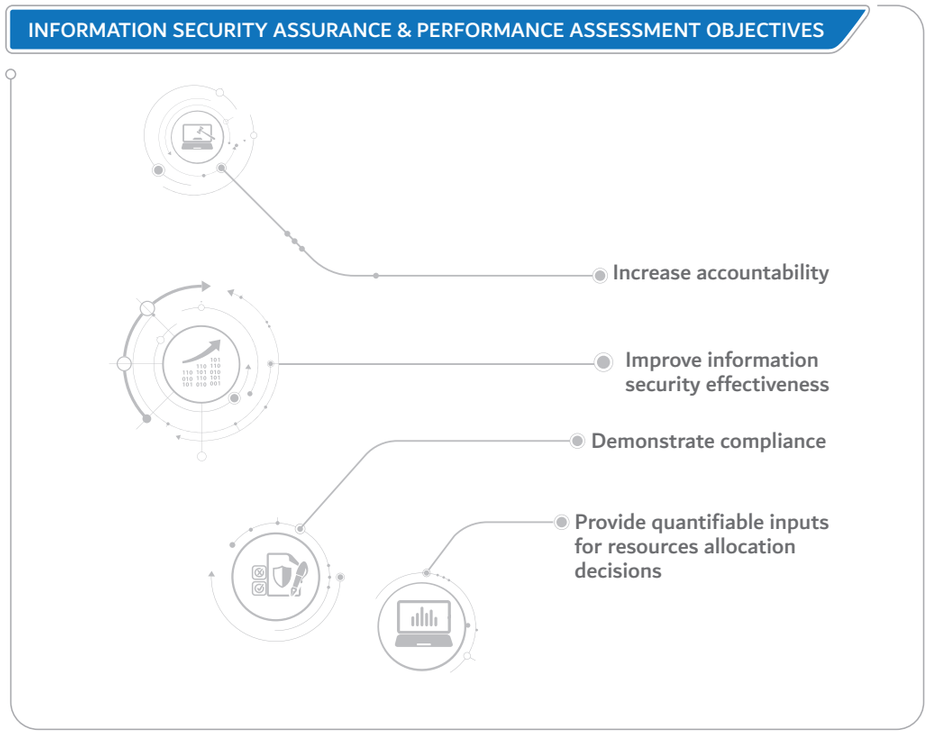
To ensure the development, selection and implementation of information security measures which facilitate decision making and improve performance through the following:

A. Increase accountability

B. Improve information security effectiveness

C. Demonstrate compliance

D. Provide quantifiable inputs for resources allocation decisions



Main Control - 12.1 Information Security Key Performance Indicators:

Dubai Government Entity

12.1.1 Develops, selects and implements a set of Information Security Key Performance Indicators (KPIs) that are:

A. In support of the government entity strategic and operational planning processes to secure the entity's mission.

B. Integrated into the annual reporting of effectiveness of the government entity's information security controls.

C. Defined to assist in monitoring compliance with the Information Security Regulation.

D. Reviewed regularly and used to support policy, resources allocation, budget decisions, and as an assessment of information security program posture and operational risks.

E. Used to address issues and deficiencies and take corrective actions such as revising policies and procedures, or provide information security trainings for employees.

F. Built from inputs of a variety of entity's stakeholders, such as IT operations, incident response team, human resources, physical security team, or others using different data sources, such as risk assessments, penetration testing, and continuous monitoring.

G. Yielding quantifiable information for comparison purposes, while using formulas for analysis, and tracking changes using the same point of reference. Percentage, average or absolute numbers can be used, depending on the activity being measured.

H. Measured over consistent and repeatable information security processes.

12.1.2 Integrates information security measurements and Key Performance Indicators (KPIs) in entity's business processes and assigns business process owners the responsibility of achieving such measures.

12.1.3 Approves the entity's information security measurements and Key Performance Indicators (KPIs) by the higher management of the entity.

12.1.4 Conducts periodic reviews on the results of information security measurements in order to ensure continual improvement of information security program within the entity.

12.1.5 Records actions and events that could have an impact on the effectiveness or performance of the Information Security Regulation.

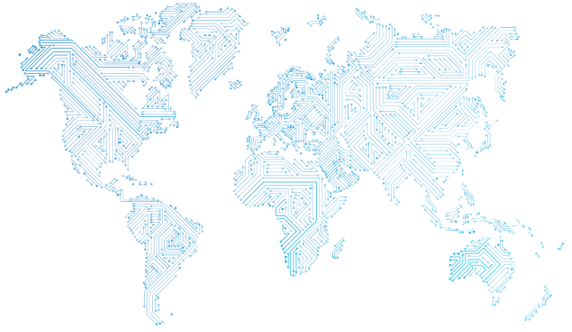
Main Control - 12.2 Information Security Dashboard:

Dubai Government Entity

12.2.1 Implements, as necessary, an integrated dashboard (or incorporates into an existing entity Performance Measurement tool) for combining all measured information security KPIs to be reviewed and monitored in a periodic manner, by the senior management and the responsible stakeholders, in order to ease the decision making process, and facilitate the overall planning for the information security program/management system.

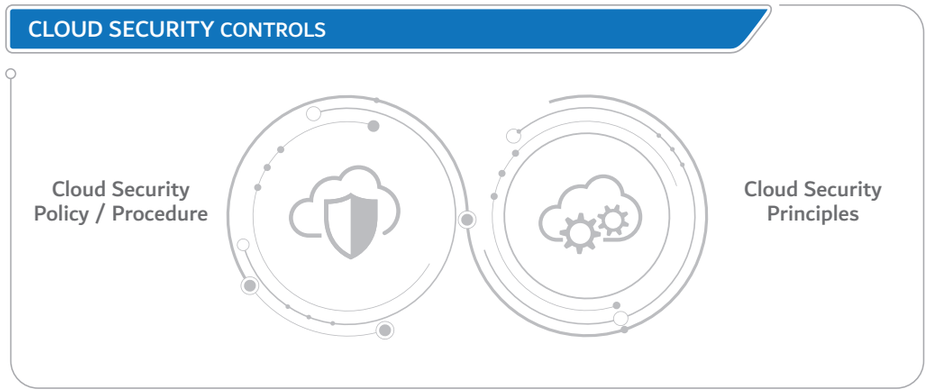
INFORMATION SECURITY
REGULATION

DOMAIN 13
Cloud Security



OBJECTIVE:

To set controls for mitigating risks associated with cloud computing and usage of cloud services.



Main Control - 13.1 Cloud Security Policy / Procedure:

Dubai Government Entity

13.1.1 Develops, distributes and maintains a formal cloud security policy that addresses the entity's requirements for overall cloud management process and outlines roles and responsibilities of relevant stakeholders.

13.1.2 Develops, distributes and maintains a cloud security procedure that provides implementation details for establishing and managing secured cloud service environment.

13.1.3 Conducts periodic reviews of cloud security policy and procedure or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Main Control - 13.2 Cloud Security Principles:

Sub Control - 13.2.1 Data Location:

Dubai Government Entity

13.2.1.1 Prevents handling and storing classified data with a Cloud Service Provider (CSP), outside the legal jurisdiction or geographical boundaries of the United Arab Emirates, including for CSP's Backup or Disaster Recovery purposes.

Sub Control - 13.2.2 Data Classification and Handling:

Dubai Government Entity

13.2.2.1 Defines and communicates required security controls to Cloud Service Provider (CSP) for handling of data in accordance to the applicable laws & regulations (in line with ISR Ref. 11.1 and 11.2).

Sub Control - 13.2.3 Architecture and Deployment Model:

Dubai Government Entity

13.2.3.1 Ensures adequate cloud security controls are implemented by Cloud Service Provider (CSP) as per architecture and deployment model approved by the entity.

Sub Control - 13.2.4 Service Agreements:

Dubai Government Entity

13.2.4.1 Ensures through a formal agreement that the Cloud Service Provider (CSP) has no ownership rights on the stored data regardless of the format or storage medium.

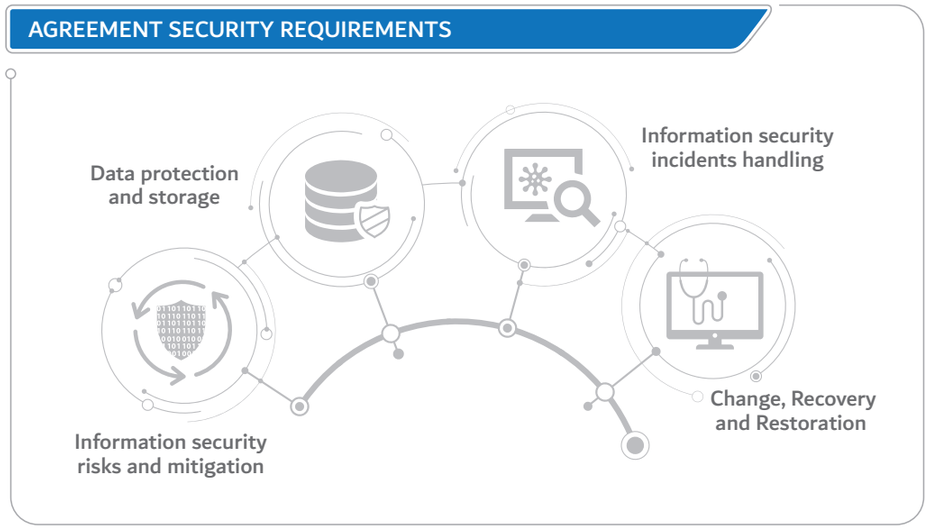
13.2.4.2 Develops and maintains a formal agreement with Cloud Service Provider (CSP) addressing the following information security requirements as a minimum:

A. Information security risks and mitigation

B. Data protection and storage

C. Information security incidents handling

D. Change, Recovery and Restoration



Sub Control - 13.2.5 Data Portability and Continuity:

Dubai Government Entity

13.2.5.1 Ensures that Cloud Service Provider (CSP) has the adequate measures and processes to support data portability whenever the entity decides to moving its data.

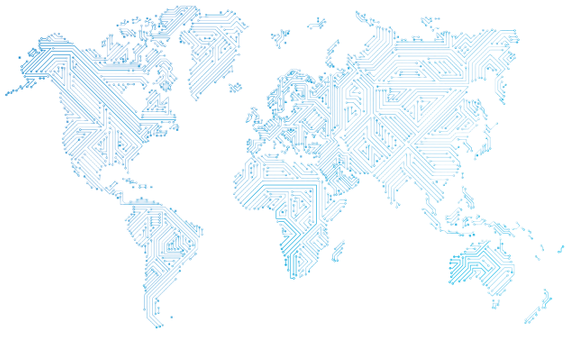
13.2.5.2 Ensures proper cloud security controls are implemented by Cloud Service Provider (CSP), addressing entity's requirements for periodic testing of the continuity and disaster recovery plans and communicating the results to entity.

Sub Control - 13.2.6 Compliance and Monitoring:

Dubai Government Entity

13.2.6.1 Conducts periodic reviews or audits to verify Cloud Service Provider's (CSPs) compliance with the applicable security policies and contractual requirements.

ORGANIZATIONS AND WORKS CONSULTED IN BRIEF



An extensive research was conducted on existing information security standards, regulations and frameworks in the course of drafting and revising Dubai Government Information Security Regulation. Pertinent information security documents were identified and consulted from the following organizations among others:

- The International Organization for Standardization (ISO)
- British Standards Institute (BSI)
- National Institute of Standards and Technology (NIST)
- Information Security Forum
- Payment Card Industry (PCI) Standards Council
- Information Technology Governance Institute (ITGI)
- Information Systems Audit and Control Association (ISACA)
- Organization for Economic Cooperation and Development (OECD)

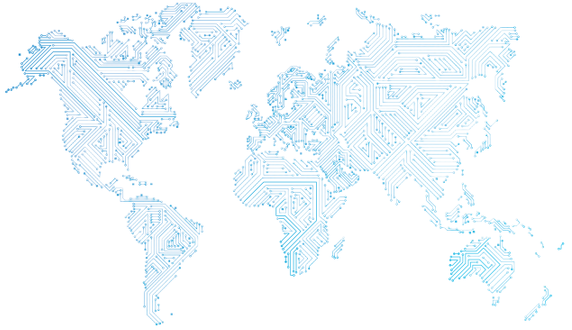
Further various versions of several standards, regulations and frameworks related to information security were considered for maintaining the Information Security Regulation, including but not limited to:

- ISO/IEC (The International Organization for Standardization / The International Electrotechnical Commission) standards,
- BSI (The British Standards Institute) standards,
- PCI (The Payment Card Industry) council standards,
- COBIT (Control Objectives for Information and Related Technology) framework,
- ITIL (Information Technology Infrastructure Library) framework,
- SOX (Sarbanes-Oxley Act),
- COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework.

Additionally, various official government sites from different countries were examined through secondary research in order to gather the publicly available existing information security policies and practices.

Hence, the Dubai Government Information Security Regulation was formalized pursuant to Resolution No. 13 of 2012 based on leading information security regulations, frameworks, policies and practices. Further, based on Dubai Law No. 11 of 2014, DESC has taken over the responsibility of maintaining and continuously improving the Information Security Regulation (ISR) in order to address the latest information security practices and related control requirements.

APPENDIX **A**
DEFINITIONS



Access control:

Access control is a mechanism to enable authorized people to access entity resources (physical and logical) while preventing unauthorized people from doing the same.

Access privileges:

Access privileges refer to the level of access granted to a user to perform his/her job duties.

Accountability:

Accountability means that people is responsible for their action. This can be achieved through audit trails and non-repudiation.

Acquisition:

Acquisition is a process defined by a series of phases that may include conceptualization, initiation, design, evaluation, development, testing, production, modification and disposal of services and systems.

Assets:

Assets are economic resources. It is anything tangible or intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value.

Assurance:

Assurance is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

Audit Log (Trails):

A security-relevant sequential record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Authentication:

Authentication is the act of verifying a claim of identity. It is usually one or more of the following: something you know (password), something you have (identification card) or something you are (finger print).

Authorization:

Authorization determines what a subject can do on the system. Authorization happens right after identification and authentication.

Availability:

Part of the Information Security Triad; availability means that information should be available when it is needed.

Awareness:

Awareness is the knowledge and attitude members of an entity possess regarding the protection of the physical and, especially, information assets of that entity. Many entities require formal security awareness training (including handling threats related to social engineering) for all workers when they join the entity and periodically thereafter, usually annually.

Best practices:

A best practice is a technique, method, process, activity, incentive, or reward that is believed to be more effective at delivering a particular outcome than any other technique, method, process, etc. when applied to a particular condition or circumstance.

Business Continuity Planning (BCP):

Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an entity will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.

Business impact:

Business impact is defined as the damage implications that are caused by an event. Business Impact analysis looks at whether that impact is acceptable by the stakeholders or not.

Business Impact Analysis (BIA):

BIA is a process used to determine the effect of an interruption of services on each business unit and the organization as a whole. The analysis can provide information on the short and long term effects of a disaster on such factors as loss of money, reputation and services provided.

Bring Your Own Device (BYOD):

Bring your own device, (also called as bring your own technology (BYOT), bring your own phone (BYOP), and bring your own Personal Computer (BYOPC)—refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

Certification and accreditation process:

It is a systematic procedure for evaluating, describing, testing and authorizing systems prior to or after a system is in operation.

Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Accreditation is the official management decision given by a senior official to authorize operation of an information system and to explicitly accept the risk to the entity's operations (including mission, functions, image, or reputation), entity assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Change management:

Change management is a formal process for directing and controlling alterations to the information processing environment. The objectives of change management are to reduce the risks posed by changes to the information processing, environment and improve the stability and reliability of the processing environment as changes are made. The change management process ensures that a change is: Requested Approved, Planned, Tested, Scheduled, Communicated, Implemented, Documented and Reviewed after the change.

Classification:

Classification means assigning categories to assets on pre-set criteria. In Information security classification is used to categorize information assets in terms of sensitivity to protect it from unauthorized access, use, disclosure, disruption, modification or destruction.

Classified Data

Information assets / material or data that an entity claims as sensitive, secret or confidential that requires protection of its confidentiality, integrity, or availability. Access to these information is restricted to people, process or other parties.

Cloud Computing:

Cloud Computing is a form of information and communication technology sourcing and delivery model that enables convenient, on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released.

Cloud Security

Refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Consists of all measures, practices and guidelines that must be implemented to enable a secure cloud architecture and to protect a cloud computing environment (SaaS, PaaS, IaaS etc.).

Cloud Service Provider:

An entity that provides cloud based platforms, infrastructure, application, and security or storage services for another entity/organization, usually for a fee.

Competent Resources

Skilled information security professional. A Competent Resource having the capability and ability to deliver training and awareness to the entity's staff and other users to support the entity's information security program.

Compliance:

Compliance is the act of adhering to, and demonstrating adherence to, a standard or regulation (international or internal).

Confidentiality:

Part of the Information Security Triad; confidentiality means the nondisclosure of certain information assets expect to an authorized person as per the classification level of that asset.

Configuration management:

Configuration management is an IT service management process that tracks all the individual configuration items (IT Assets) in an IT system with maybe be as simple as a single server or an entire IT department.

Conflict of Interest

A situation in which a person is in a position in an entity, to derive personal or professional benefit from actions or decisions made in their official capacity.

Critical Information Assets

An asset that has important business information and is essential to meet the business objective and related processes. It can exist in many forms and has value that is worth protecting these are essential to the entity's business and can cause major adverse impacts if their availability is interrupted, if modified/lost / destroyed or if disclosed to unauthorized parties or processes.

Cryptography:

Cryptography is the concept consisting of two parts. The process of transforming usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption.

Custodian:

A custodian is defined as an individual or entity that has approved responsibility for maintaining an information asset.

Data Portability

Concept to protect users from having their data stored in «silos» or closed platforms, thus subjecting them to lock-in. Portability refers to the ability to move data among different application programs, computing environments or cloud services or service providers.

Disaster:

Disaster is the tragedy of a natural or human-made hazards (a hazard is a situation which poses a level of threat to life, health, property, or environment) that negatively affect society or environment.

Dubai Government Entities/Entity:

Any organization legally established by Dubai Government with well-defined roles and responsibilities, including but not limited to, authorities, departments, councils, committees, etc.

Evidence:

Evidence is everything that is used to determine or demonstrate the truth of an intrusion or breach to an information system.

External Parties

An individual or organization that deals with the entity through a business relationship and has access to entity's information or an information asset.

Framework:

A framework is the combination of guidelines and structured processes that address a complex issue. The framework establishes policies and practices to provide general guidance on matters affecting information security.

Fraud:

Fraud is an intentional deception made for personal gain or to damage another individual or entity.

Governance:

Information Security governance is a subset of enterprise governance that provides strategic direction, ensures objectives are achieved, manages risk appropriately, uses entity resources responsibly, and monitors the success or failure of the enterprise security program / management system.

Incidents:

An incident can be thought of as violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Information:

Depicts any government related information, which can exist in many forms, such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

Information Asset Owner:

The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of an information asset. The term 'owner' does not mean that the person actually has any property rights to the asset. Routine tasks may be delegated, e.g. to a custodian looking after the asset on a daily basis, but the responsibility remains with the owner.

Information Exchange

Act of giving and receiving information / data or transmission/transfer of classified information (electronic or physical) internally within the entity, or externally with any external parties.

Information security:

The act of protecting information that may exist in any form, whether spoken, written, processed or transmitted electronically, etc. from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities.

Information systems:

Any computerized system used for managing and processing any government related information within a single entity or crossing multiple entities.

Information Processing:

Information processing entails any activity on the information including, but not limited to, creation, modification, deletion, storage, transmission, replication, encryption, decryption, etc.

Information processing facilities:

An information processing facility is defined as any system, service, or infrastructure, or any physical location that houses these things. A facility can be either an activity or a place; it can be either tangible or intangible.

Integrity:

Part of the Information Security Triad; integrity means that data cannot be modified without authorization, intentionally or unintentionally.

Inventory:

Inventory is a list of goods and material owned by an entity – inventory recording could be in the form of an asset register.

Information Leakage:

Leakage is allowing sensitive or confidential information to become known by someone not authorized to view such information.

Logical access control:

Logical access control refers to the collection of policies, procedures, entity structure and electronic access controls (technology) designed to enable safe access to computer software and data files as well as to the network.

Malicious attack:

Malicious attack is an attempt to infiltrate a computer system without the owner's informed consent to make it unavailable, steal information or use it to attack other computers using a malicious software or code. (This includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crime ware, rootkits, and other malicious and unwanted software).

Media Library:

A secure Information Technology repository in which an organization's definitive, authorized versions of software media are stored and protected.

Need to Know Concept:

An administrative process certifying that a given individual requires access to specified private information in order to perform his or her assigned duties.

Network Routing:

Process of selecting paths in a network along which to send network traffic.

Network Traffic Devices:

Components used to connect computers or other electronic devices together so that they can communicate such as hub, switch, router, and modem.

Non-repudiation:

Non-repudiation implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. An example to non- repudiation is using digital signature.

On-line transaction

Entity's Software, data, and other information being made available or allowed to be accessed using a publicly available system, typically using internet.

Physical access control:

Physical access controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

Policy:

An information security related document written and maintained to provide governing statements regarding any information security key process, through setting the rules for expected behaviour by users, systems administrators, management, and security personnel; authorize security personnel to monitor, probe, and investigate; define and authorize the consequences of violation; define the entity consensus baseline stance on security; help minimize risk; and help track compliance with regulations and legislation.

Privacy:

Privacy is the ability of an individual or group to stop information about themselves from becoming known to people other than those they choose to give the information to.

Process / Procedure:

An information security related document; adjunct to policy and written to give step-by-step directions on the 'how' of carrying out or implementing the policy statements.

Recovery point objective:

It is the maximum tolerable period in which data might be lost from an IT service due to a major incident.

Recovery time objective:

The duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Residual Risks:

The remaining risk after treatment of risk or implementing a risk response, as approved by management.

Risk:

Risk is the quantifiable likelihood of potential harm that may arise from a future event.

Risk acceptance:

Risk acceptance describes an informed decision to accept the consequences and likelihood of a particular risk.

Risk analysis:

Risk analysis is a technique to identify and assess factors that may jeopardize the success of a project or achieving a goal. This technique also helps to define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the entity.

Risk assessment:

Risk assessment is a step in the risk management process to determine the qualitative and quantitative value of risk in relation to a recognized threat. Quantitative risk assessment requires calculations of two components of risk; R, the magnitude of the potential loss L, and the probability P; that the loss will occur.

Risk management:

The process of analyzing risk and exposure through identification, assessment and prioritization followed by monitoring and applying controls to best handle the exposure.

Risk treatment:

Risk treatment – also known as risk control – describes the part of risk management in which decisions are made about how to treat risks that have been previously identified and prioritized. Options for risk treatment may include risk avoidance, risk reduction, risk transfer or risk acceptance.

Security or Information Security Architecture

Describes the structure, components and topology (connections and layout) of security controls within an enterprise's IT infrastructure. The security architecture or the Framework shows how defense in depth is implemented and how layers of control are linked in implementing security controls in the entity's IT environment.

Security breach:

A Security breach is an external act that bypasses or contravenes security policies, practices or procedures.

Security control:

Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks. They could be preventive, detective or corrective.

Security measures:

Preventive measures taken against possible danger or damage occurs.

Segregation of Duties:

Segregation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users.

Senior Management:

A layer of management in an entity whose primary job responsibility is to monitor activities of subordinates as well as the day to day operations; for example Managers/ Directors of HR, IT

Finance, Marketing, Engineering, etc. while reporting to upper management such as CEO or Director General.

Stakeholders

A person, group or organization that has interest or concern in an organization. Stakeholders can affect or be affected by the organization's actions, objectives and policies.

Systems Acquisition/Development Life Cycle:

A process of buying or creating or altering information systems, and the models and methodologies that people use to develop these systems.

Systems/application source codes:

Any collection of computer instructions written using computer language.

Threat:

Threat is the expressed potential for the occurrence of a harmful event such as an attack. It could be any party with the intent and capability to exploit vulnerability in an asset such as a malicious hacker or a disgruntled employee.

User ID:

A name used to gain access to a computer system.

Virtualization Techniques

Creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system (OS), storage device, or network resources and can be view as part of an overall entity IT environment

Vulnerability:

Vulnerability is weakness in an asset that can be exploited