حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

DESC ICS Standard

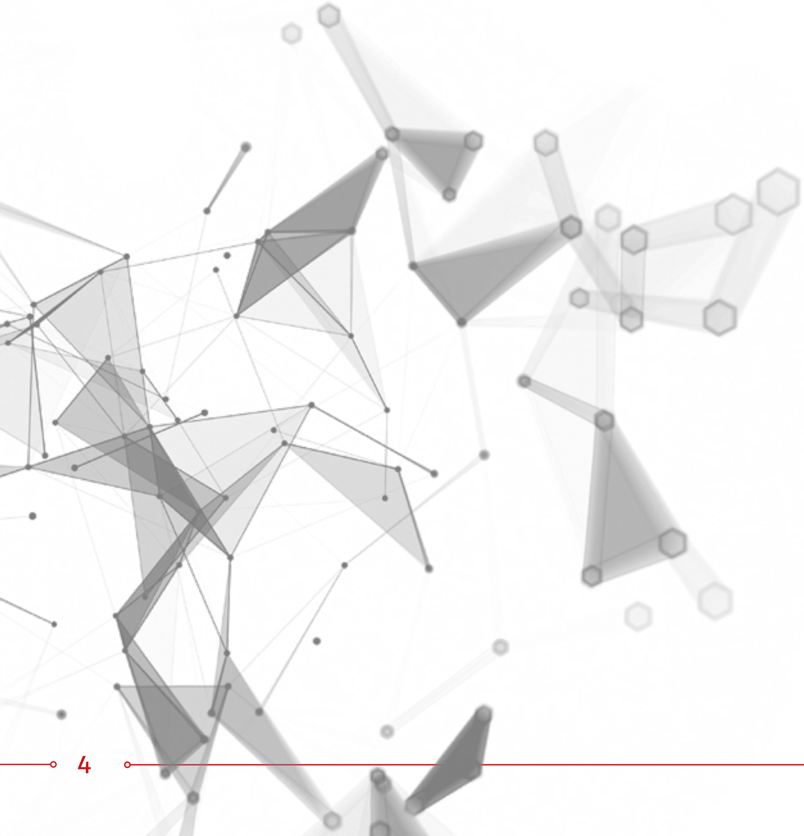
VERSION 1.0

حكومة دبي
GOVERNMENT OF DUBAI

DESC
ICS
STANDARD

VERSION 1.0

TABLE OF CONTENTS



ACKNOWLEDGMENT

Information Security Regulation (ISR) for Industrial Control systems, also referred to as Operational technology for the Critical Infrastructure operators 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 for ICS standard encompasses several cybersecurity domains composed of specific controls and sub-controls, to guide the critical infrastructure operators to address cyber risks related to ICS/OT and is closely aligned with other International ICS security related Standards reflecting Dubai Government's acknowledgement and recognition of the cybersecurity best practices stated therein. The ICS standard also includes distinctive clauses reflecting specific requirements within the context of The Dubai Government.

This standard is applicable to Dubai government and semi-government entities that operate critical infrastructure and/or Industrial Control Systems (Operational Technology).

To align with globally followed leading practices, the controls in this standard are based on, and benchmarked with several other standards which are as follows:

- Information Security Regulation V2.0 (DESC)
- NIST 800-82 (NIST)
- IEC 62443 (ISA 99)
- ISO 27001: 2013

INTRODUCTION

Digitalization and automation of industrial processes has helped entities to enhance their operations and increase their output/production efficiently. With ever increasing presence of commercial off the shelf technologies replacing manufacturer proprietary systems in the ICS environment, it has helped organizations scale up their operations, but at the same time has resulted in a drastic increase of the attack surface area in the ICS environments. With businesses requiring their ICS networks & systems to have inter-connectivity internally and, on some occasions, externally, to non-ICS networks (deemed as less-secure), the ICS systems and networks are exposed to increased no. of threat & vulnerabilities, which subsequently leads to an increase in the risk of a cyberattack. ICS systems & networks when compromised due to a cyberattack will not only cause disruption of operations & loss of production but can also lead to health and safety hazards.

Even if most of the ICS systems today comprise of technologies adopted from the conventional IT systems, yet the risks that the ICS systems are exposed to and the impact of those risks, is vastly different from the non-ICS systems environment. For this very reason, critical infrastructure entities will need to adopt and implement suitable measures in form of controls, processes, technical solutions and practices that are best suited to address the risks that are specific to ICS.

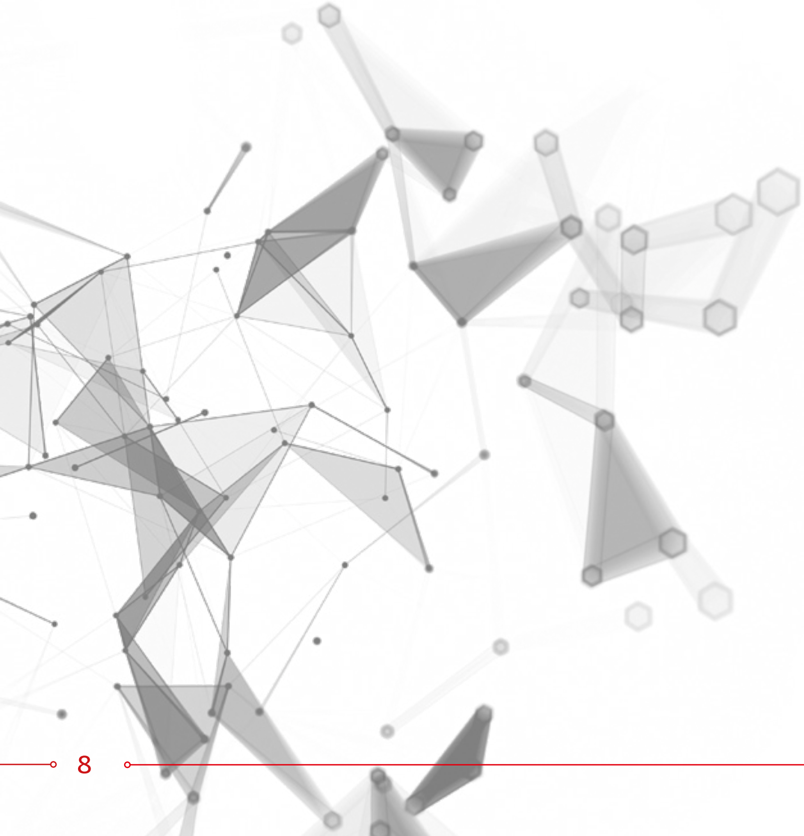
Applying conventional IT security controls & solutions for ICS can potentially lead to insufficient or ineffective protection from cyber threats, unmitigated vulnerabilities, and operations loss due to system down-time or safety hazards to personnel and plant.

The cornerstone of robust cybersecurity practices for a critical infrastructure of ICS/ OT include (but not limited to:

- Cybersecurity program established to manage the cybersecurity function and processes
- Cybersecurity governance
- Risk management, that includes a risk assessment-based approach for selecting the controls that need to be implemented

CYBERSECURITY

PROGRAM & GOVERNANCE



CYBERSECURITY PROGRAM

Establishing a cybersecurity program is critical to protect the ICS assets and services from cyberattacks. This program should be an integral part of management planning for ICS systems. This program should encourage and enforce the requirement to consider cybersecurity as part of overall operations.

This includes, establishing objectives, policies and processes, identifying ICS assets and the physical & logical perimeter of ICS environment.

CYBERSECURITY GOVERNANCE

Critical infrastructure operators/entities should establish a governance structure for effective implementation of cybersecurity program, this shall include:

Cybersecurity steering committee, whose role is to manage and monitor all cybersecurity initiatives and operations within the organization, provide resources for implementing cybersecurity program and reporting to stakeholders on key areas.

Defining the roles and responsibilities of cybersecurity team/personnel. The roles and responsibilities should be clearly defined to manage the day to day cybersecurity operations. Dedicated personnel/resources with sufficient & relevant skills in carrying out various ICS cybersecurity operations should be available on full time (recommended) or as-needed basis.

RISK MANAGEMENT

Critical infrastructure operators/entities should have an effective risk management strategy that includes carrying out comprehensive risk assessments on a periodic or as-needed basis on their ICS environment to identify the risks that the organization and its ICS systems are exposed to. Based on an entity defined risk assessment methodology or risk assessment technique, the risk levels should be determined and control requirements from this standard should be selected for implementation, to bring down the risk to acceptable levels.

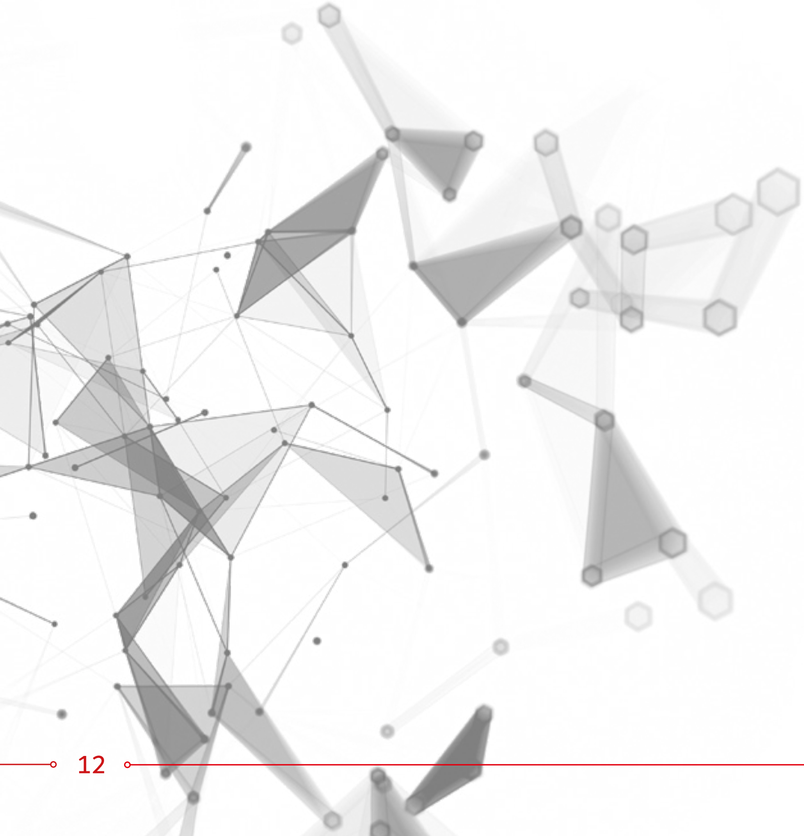
The selection of controls and the extent of implementation of corresponding solutions (deploying software, hardware, etc.) should be based on the risk determined. Entities are encouraged to adopt threat modelling-based risk assessment (more effective to identify 'common mode impact' where multiple ICS devices/systems that are connected or related get impacted by a single event of cyberattack) or, where that's too complex, a detailed asset-based risk assessment could be performed.

The results of the risk assessment should be documented in a risk register, which could contain the following details:

- Risk statement
- Asset class impacted
- Threats and threat scoring
- Vulnerability and vulnerability scoring
- Current risk level/rating (this is not same as inherent risk, which is not needed to be recorded)
- Applicable controls (from this ICS Security standard)
- Summary of risk remediation activities
- Risk owner
- Remediation responsibility and proposed close date
- Residual level (after the controls would have been successfully implemented to mitigate/reduce the identified risks)

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

PHYSICAL AND LOGICAL PERIMETER (BOUNDARY) OF ICS



PHYSICAL AND LOGICAL PERIMETER (BOUNDARY) OF ICS

The process of applying security measures or controls in an ICS environment starts with identifying all the assets, which include all automation/computerized assets, that support or monitor operations in ICS environment like, but not limited to – SCADA servers, DCS, HMIs, PLCs, RTUs, MTUs, network devices, control rooms, operator stations, database servers, physical & virtual servers/workstations, remote sites, marshalling cabinets, safety instrumentation systems, protective relays, cabling, sensors, actuators, valves, etc. All the assets identified should be documented, and asset criticality analysis should be performed.

Further, all interconnections should be documented, as accurately as possible, listing the assets that are interconnected, connection type and reason for connectivity.

Once the ICS assets are identified and interconnections mapped, the organization should then use the information to define the physical and logical perimeters, which then become the scope for their cybersecurity program (cybersecurity controls & measures would need to be applied, based on the risk applicability, across all assets within the perimeter/boundary).

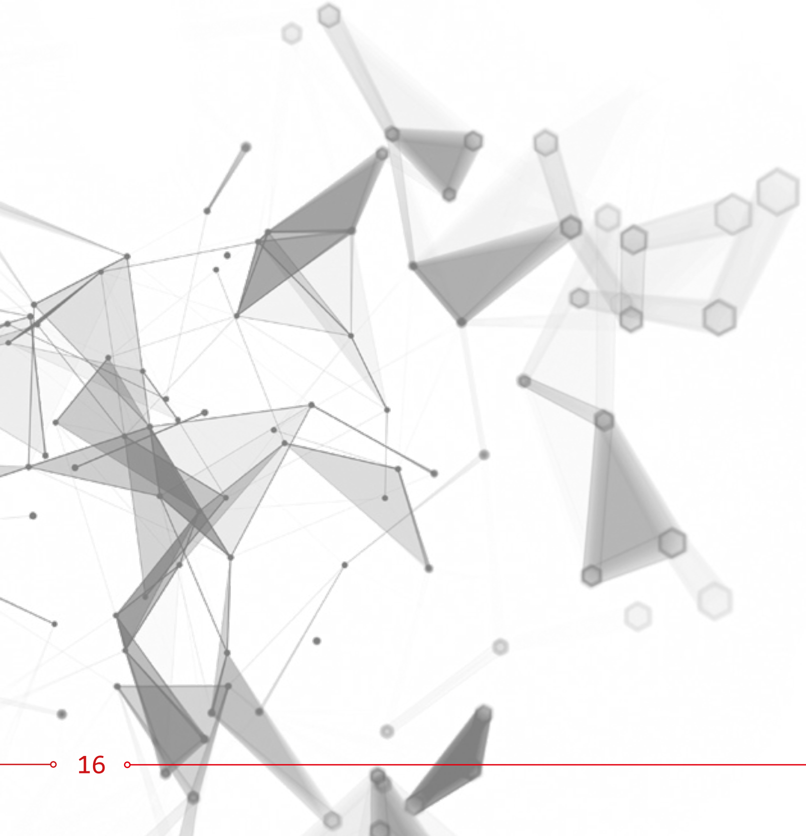
Note 1: An organization can have multiple sites (remote sites, sub-stations, etc.), **if they exist on a single ICS network or have network interconnectivity, shall be considered as an integrated logical perimeter.**

Identifying and determining the perimeter is very crucial to the protection of critical assets, since it aids in implementing controls across the entire environment, thereby eliminating the risk of unidentified assets and vulnerabilities.

Note 2: It should be noted that establishing objectives, policies and processes, controls for ICS assets and the physical & logical perimeter of ICS environment has to be eventually integrated with entity level Information Security Management Program, in alignment with Information Security Regulation (ISR). This transition document is provided to enable ICS specific environment to focus on related risks and controls and help implement the required controls quickly. However, these controls will be integrated and incorporated as additional security domain in the next release of ISR version. Domain 1 - Information Security Management and Governance.

DOMAIN 1

INFORMATION SECURITY MANAGEMENT AND GOVERNANCE



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:

- Aligning Information security with the entity strategic direction
- Ensuring information security objectives are achieved
- Managing risks appropriately
- Using entity resources responsibly
- Continuous monitoring of the information security program

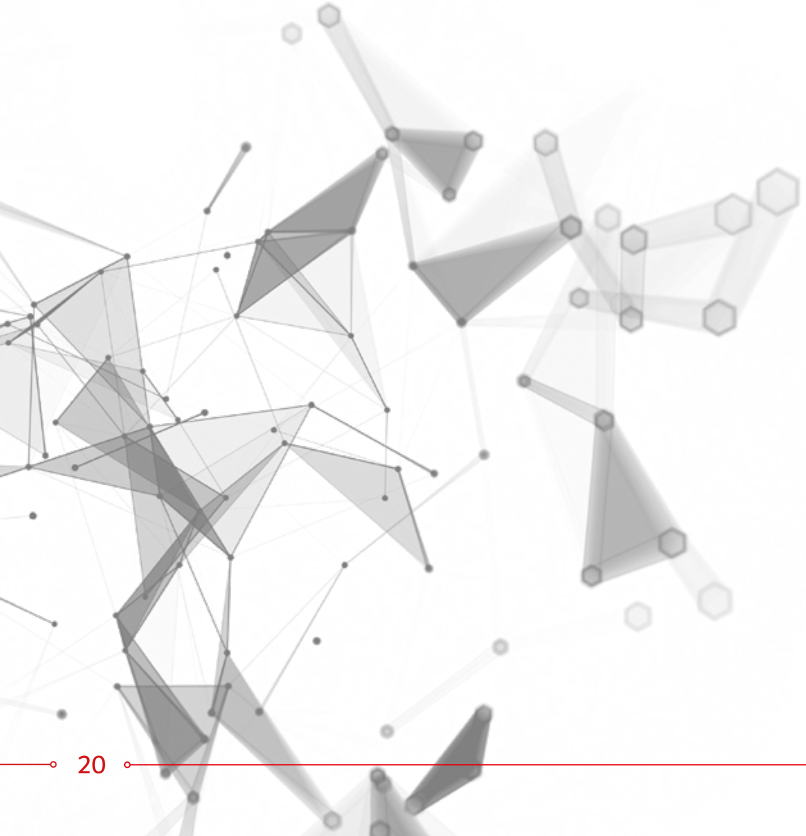
Information Security Management and Governance related controls specified in the Information Security Regulation (ISR) V.2.0 should be implemented covering the following:

- Roles and Responsibilities of Information Security
- Information Security Policy
- Technical and Operational Policies
- Information Security Awareness and Training

- Confidentiality Agreements
- Relations and Sustainability of Information Security
- Information Security Management and Governance

DOMAIN 2

ICS ASSETS MANAGEMENT



DOMAIN 2
ICS ASSETS MANAGEMENT

OBJECTIVE:

To enable visibility of the ICS environment by identifying, recording, reviewing and proper handling of ICS assets thereby enabling appropriate application of security controls to protect and avoid theft, loss of information, attacks etc.

1. Main Control - ICS Assets Management

Dubai Government Organization

1.1. Develops, distributes and maintains an ICS asset management policy and procedures that are aligned with the organization wide information asset management policy and procedure for the identification, management and protection of ICS assets in line with applicable laws and regulations.

1.2. Identifies, documents, and maintains an asset register of all critical ICS assets for the entire ICS environment, including the related ICS facilities and components, such as PLCs, RTUs, SCADA/DCS servers, engineering stations, operators stations, network devices, software assets, people assets, physical assets, etc. and consider other details such as, asset classification, physical location, license details, business value, and any other necessary information that may be required to avoid risks and recover from disasters.

1.3. The organization appoints designated employees with the responsibility to perform periodic review of the asset management register and enforce policies and procedures to periodically update the register for accuracy

1.4. In case of utilizing asset inventory tools, the organization ensures appropriate testing of the tool in non-production environments prior to deployment in the ICS production environment.

1.5. Keeps inventory of all physical access devices owned by the organization.

2. Main Control - ICS Assets Ownership/ Custodianship:

Dubai Government Organization

2.1. Establishes and implements ICS asset ownership policy, where ICS assets are identified with an owner. Business processes, services, applications, ICS systems, or set of data are examples of assets that ownership should be allocated to.

2.2. Assigns the ICS assets owner the responsibility of ensuring that classifications of ICS assets are carried out based on the sensitivity of operations.

2.3. Assigns the ICS assets owner the responsibility of defining the access control (physical & logical) to the ICS assets and ensuring periodic review of access in accordance with assigned classification level and the organization's access control policy.

2.4. Assigns the owner the responsibility of maintaining the day to day operational tasks related to the ICS assets, while considering the higher authority of the assets by the owners.

3. Main Control - ICS Assets Classification:

Dubai Government Organization

3.1. Defines and implements a classification scheme/ process for ICS assets to be used within the organization based on ICS assets criticality, value, legal and protection requirements, etc. in line with applicable laws and regulations.

3.2. Develops, distributes and maintains ICS classification policy and related procedures in line with applicable laws and regulations, for e.g. data classification regulations provided by the Emirate of Dubai

3.3. Ensures classification of ICS assets based on criticality. The organization defines criticality of the ICS assets by deriving the Availability, Integrity and Confidentiality ratings of individual ICS systems and based on the impact to the safety functionalities of the system.

3.4. Ensures periodic asset review for enabling an update of the Asset register.

4. Main Control - ICS Assets Labeling and Handling:

Dubai Government Organization

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

4.2. Develops, distributes and maintains procedure for the ICS assets labeling and handling requirements.

5. Main Control - Disposals of ICS Assets:

Dubai Government Organization

5.1. Identifies and implements the required safety and security measures prior to the disposal of ICS assets based on their value, criticality and sensitivity. This should be applied to ICS assets that either reached the End of life or are no longer needed for operations.

5.2. Develops, distributes and maintains clear procedure for the process of disposal of ICS assets, which includes irretrievably erasing all information including any code or configurations before securely physically disposing such assets.

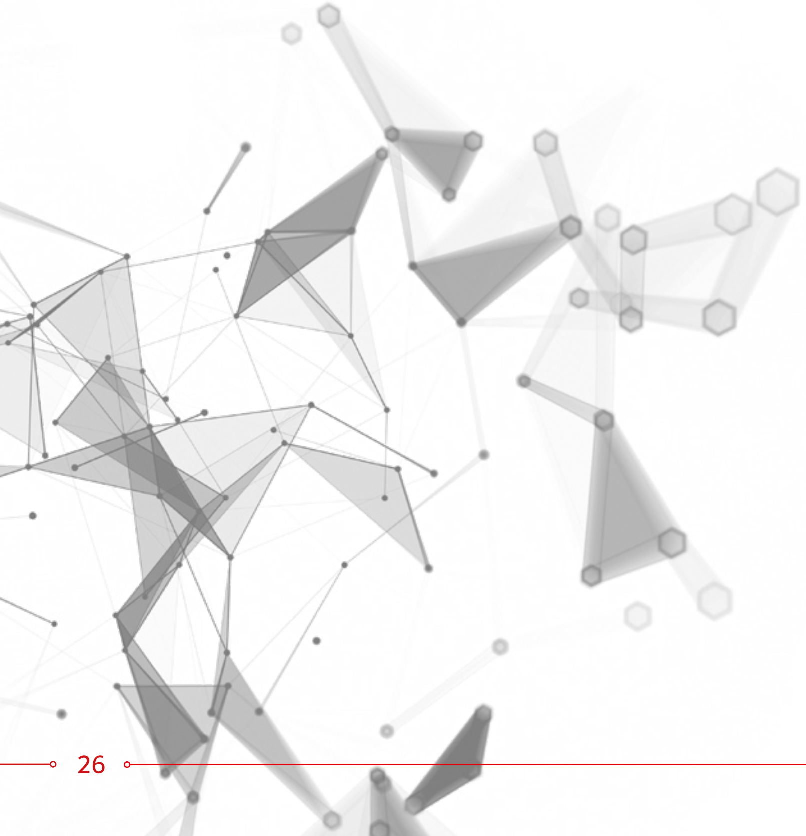
6. Main Control - ICS Assets Responsibility:

Dubai Government Organization

6.1. Develops, distributes and maintains an acceptable use policy governing the use of ICS assets including restricting usage of personal devices in or near ICS environment.

DOMAIN 3

ICS SECURITY AND RISK MANAGEMENT



DOMAIN 3
ICS SECURITY AND RISK MANAGEMENT

OBJECTIVE:

To identify risks to the ICS environment and its assets by developing an astute understanding of the ICS operations and processes to derive suitable risk treatment strategies and develop a platform for enabling adequate mitigation of identified risks to the ICS environment, for an effective overall risk management process.

1. Main Control – Risk Assessment Methodology & Planning:

Dubai Government Organization

1.1. Develops a risk assessment methodology that aligns with the requirements of the organization’s information security program, covering the life cycle of the ICS asset (from identification till disposal).

1.2. Determines a periodic plan for conducting the risk assessment across the organization’s operational/production environments.

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

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

1.5. Plans and implements a periodic awareness of the risk assessment program across the organization.

2. Main Control - Risk Assessment:

Dubai Government Organization

2.1. Conducts & maintains a detailed risk assessment addressing various types of risks (E.g. Security, Health & Safety, Environmental, etc.), for the identified critical information assets, in accordance with the approved risk assessment methodology.

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

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

2.4. Documents the risk assessment results in a risk register, which is approved officially by higher management. The risk register shall be updated on a continuous basis.

3. Main Control – Risk Treatment and Mitigation:

Dubai Government Organization

3.1. Selects the risk treatment plans (mitigate, avoid, transfer, etc.) for the identified risks, approved by the higher management.

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

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

4. Main Control - Risk Acceptance:

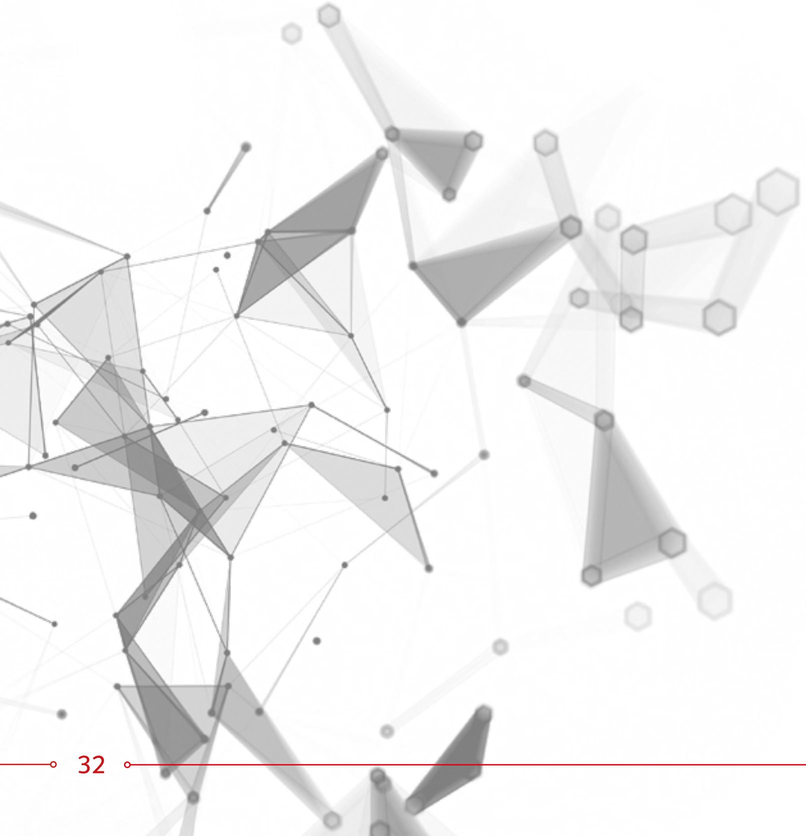
Dubai Government Organization

4.1. Documents the residual non-treated risks with justifications and gets it signed off by higher management.

4.2. Provides the detailed plan for treatment within agreed timelines.

DOMAIN 4

INCIDENT AND PROBLEM MANAGEMENT



DOMAIN 4
INCIDENT AND PROBLEM MANAGEMENT

OBJECTIVE:

To define operational guidelines pertaining to effective identification and handling of ICS Cybersecurity incidents to minimize the adverse impact on plant operations.

1. Main Control – Incident Management Planning:

Dubai Government Organization

1.1. Develops, distributes and maintains a documented policy and procedure for the management and handling of ICS security incidents.

1.2. Establishes a technology capability (Incident Response Team) to identify, analyse, eliminate, prevent and recover from the ICS security related incidents ranging from process IT, automation, ICS operations & maintenance across the organization.

1.3. Performs regular (quarterly) exercises with the Incident Response Team to exercise & execute effective handling of ICS security incidents.

1.4. Develop mechanisms to detect, analyse, contain, eradicate and recover from ICS Cybersecurity incidents.

1.5. Performs classification, as per a documented classification scheme, of various types of ICS Incidents so that the potential impact and suitable mitigation approach is mapped.

1.6. Ensures the distribution, review and approval of the Incident response plan from relevant operation teams and Stakeholders.

1.7. Perform Post-mortem or Lessons learnt activities after incidents to improve the process and ensure that control updates are communicated to the control owners.

2. Main Control – ICS Security Incident Reporting & Escalation:

Dubai Government Organization

2.1. Assigns responsibility to designated employees or users dealing with the organization's ICS operation and information, through appropriate means, for reporting promptly any observed or suspected ICS security incidents or weaknesses in systems or services, to the responsible organization's team.

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

2.3. Defines timelines for reporting on identified responses and enables suitable measures for ensuring adherence to defined timeline.

2.4. Wherever feasible, the organization adopts automated reporting mechanisms thereby enabling ease and efficiency of Incident response.

3. Main Control – Evidence Gathering:

Dubai Government Organization

3.1. Implement a process to gather and retain evidences related to any ICS security incidents.

3.2. Ensure that personnel involved in incident management are trained in the correct handling of evidence.

4. Main Control - ICS Security Incidents Knowledge base:

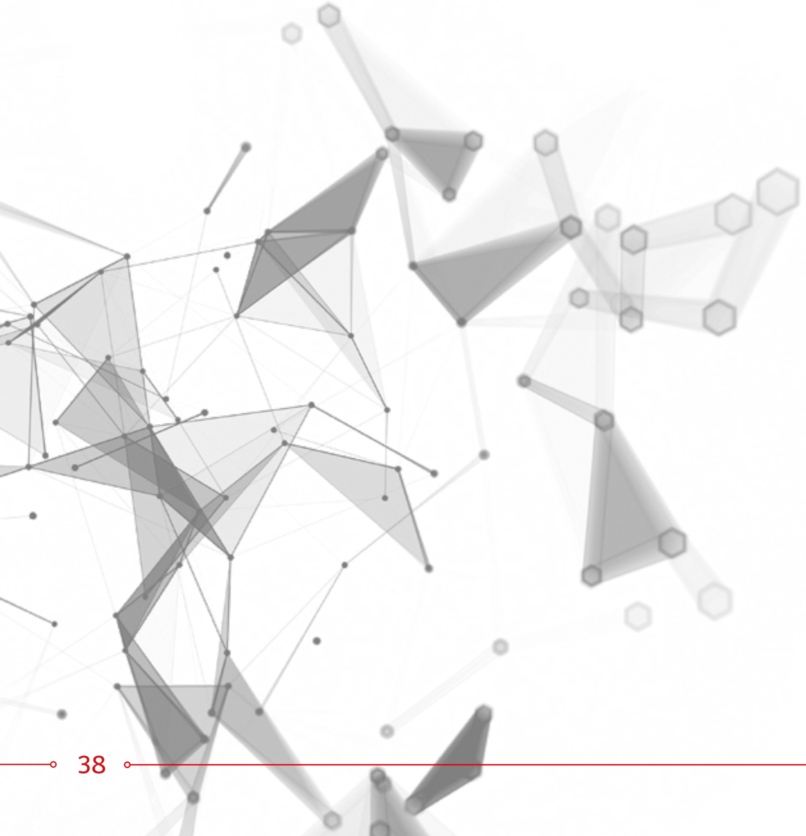
Dubai Government Organization

4.1. Develops a knowledge base from all occurred ICS security incidents, with the focus of preventing and protecting the organization ICS assets from identified risks and related incidents, which includes details of incident types and any other relevant information.

4.2. Develops a repository of current ICS security incidents that are relevant to the organization's operations and ICS environment. Performs root cause analysis of such incidents and adopts means to assure the organization of protection from such identified risks.

DOMAIN 5

ACCESS CONTROL



DOMAIN 5
ACCESS CONTROL

OBJECTIVE:

To define necessary security controls for the safeguarding of physical and logical access to the ICS systems and components.

1. Main Control - Access Control Management Policy/Procedure:

Dubai Government Organization

1.1. Develops, distributes and maintains an access control policy that addresses all security requirements for the implementation of an effective access control for ICS assets within the ICS environment of the organization.

1.2. Develops, distributes and maintains an access control procedure that provides implementation details for access control, based on role-based access control (wherever possible) to individual ICS systems and components.

1.3. Ensures the ICS security access control policy clearly defines security roles, responsibilities and necessary cross-functional coordination among teams responsible for the operation, installation and maintenance of the ICS systems and components.

1.4. Ensures periodic review and update of the Access Control policy and procedures in accordance with dynamic risks identified in the ICS environment.

2. Sub Control - Logical Access Control:

2.1. Sub control - Users Access Control:

Dubai Government Organization

2.1.1. Defines and implements a process for ICS system user registration, de-registration, and users access privileges modification, disabling or removal, etc.

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

2.1.3. Implements a unified user ID standard across the organization.

2.1.4. Implements an authentication technique for the validation of claimed identities of users regarding access being on-site and remote.

2.1.5. Develops, distributes and maintains appropriate authentication policy specific to the ICS environment (e.g. a password management policy that clearly addresses the password allocation process, ICS system users' responsibilities on passwords use and the recommended password structure, etc.).

2.1.6. Identifies the categories of ICS system users requiring regular and special privileges by ensuring the availability of the following:

a) A valid and approved access authorization.

b) Other attributes as required by the organization or associated missions/ business functions.

c) Utilization of access accounts with special privileges must be restricted for their intended purpose and only within the intended ICS systems and components.

2.1.7. Performs a periodic review of ICS users having privileged access rights on the ICS systems to ensure that the access privileges are commensurate with their job responsibilities.

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.

2.1.9. Implement security and independent monitoring controls over the usage of special or high privileged IDs within the ICS environment.

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

2.1.11. Ensures usage of shared accounts within the ICS environment only for non-administrative functions such as, functioning of operator stations, operation monitoring and analysis etc. In such cases, the organization maintains a list of users with access to the shared account login and password credentials and performs periodic reviews of user activity logs.

2.1.12. For critical operations deemed by the organization, the organization shall deploy appropriate approvals prior to execution of operation ensuring reliability and accuracy.

2.1.13. The organization enables exceptions for control 5.2.1.12; for operations mandating instantaneous response for securing plant safety, based on higher management approvals.

2.1.14. Wherever deemed appropriate, the organization ensures protection of Information confidentiality within the ICS environment, limiting access only to authorized users for both data at rest and in transit, using suitable methods such as encryption, compartmentalization, physical separation etc.

2.1.15. The organization explicitly defines ICS operational zone boundaries and deploys suitable protection measures for ensuring security of data traversing across zone boundaries.

2.2. Sub control – Network Access Control:

Dubai Government Organization

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

2.2.2. Defines a process for authorizing, activating and terminating any network connections in the organization.

2.2.3. Implement network access control tool/method for network equipment/devices connectivity detection, identification and authentication.

2.2.4. Remote access to the ICS systems should be restricted and granted only under circumstances where it is absolutely needed. Remote access should be granted only after approvals are obtained.

2.2.5. Implements authentication tool for remote access connections.

2.2.6. Manage and controls access to configuration ports on network equipment / devices.

2.2.7. Implement segregation controls on between ICS and other networks (internal, external, wireless, IP telephony, etc.).

2.2.8. Ensures deployment of Network Segmentation with restricted logical security access enabling network design simplification and isolation of network traffic within designated zones of operation.

2.2.9. Ensure the Network switches used in the ICS environment are configured with appropriate rules and the defined rule set is periodically reviewed for integrity and uniformity across the ICS environment.

2.2.10. Ensures a risk-based review of enforced security policies and traffic segregation rules on managed switches in line with necessary mitigation steps to identified risks.

2.2.11. Enables multi-factor authentication within the ICS environment wherever applicable. In particular, connections established from External/ Untrusted networks must be routed via a multi-factor authentication mechanism prior to being given access to the ICS environment.

2.2.12. Establishes network monitoring and analysis mechanisms for monitoring traffic from such untrusted network.

2.2.13. Enables remote session termination controls (Manual or automatic) such that internal users exercise the control to instantly terminate remote connections or set configurable time-slots for external users to operate within.

2.3. Sub control - Operating System Access control:

Dubai Government Organization

2.3.1. Manages and controls the use of utility programs within the ICS environment.

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

2.3.3. Implements lock-out policy.

2.3.4. Restricts connection times and persistent connections for critical ICS systems and applications.

2.3.5. Records and continuously reviews logs of administrator system IDs.

2.3.6. The organization shall also enforce users to periodically change their passwords and to ascertain the use of the same password only after a certain number of times.

2.3.7. The organization enables a mechanism to lock user accounts post a consecutive number of unsuccessful login attempts. The users should be re-enabled access only upon having prior procedures in check.

2.4. Sub Control - Remote Access Security:

Dubai Government Organization

2.4.1. Develops, distributes and maintains an ICS remote access security policy addressing remote access to the organization’s resources (remote access should be allowed only for exceptional cases based on business requirement).

2.4.2. Enforces authorization prior to remote access connections to the ICS systems/components.

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

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

2.4.5. Monitors and periodically reviews the remote access connections logs.

2.4.6. Enables multi-factor authentication for users connecting to the ICS environment from remote locations.

2.4.7. Wherever feasible, deploys bi-directional authentication for remote connections to enable stronger security control.

2.4.8. Ensures remote connections are enabled only to systems that require to be accessed remotely by users.

2.4.9. BYOD (bring your own device/personal devices) should not be allowed within ICS environment.

2.5. Sub Control - Wireless Access Management:

Dubai Government Organization

2.5.1. Develops, distributes and maintains a documented policy on the wireless network usage within ICS environment.

2.5.2. Authorizes the wireless access to the ICS network prior to any connection.

2.5.3. Implement authentication control for the wireless access.

2.5.4. Enforce security control for wireless connections to the organization's ICS network and establishes usage restrictions and implementation guidance for such use.

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

2.5.6. Monitors continuously for any unauthorized wireless access to the network.

2.5.7. Deploys mechanisms to ensure unique identification and authentication of all users over wireless communication networks.

2.5.8. Enforces wireless use restrictions, monitoring mechanisms and authentication controls for wireless utility to the ICS environment.

2.5.9. Enables mechanisms to identify unauthorized users within the ICS environment and adopts suitable reporting mechanisms to prompt timely action.

3. Sub Control - Logical Access Control:

3.1. Sub Control - Physical Access Policy and Procedure:

Dubai Government Organization

3.1.1. Develops, distributes and maintains a documented physical access policy that addresses the organization's requirements for implementing physical access controls on control rooms, maintenance rooms, engineering environments etc.

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 to be deployed within the ICS environment.

3.1.3. Enforces authorization prior to physical access to any facilities with ICS systems.

3.2. Sub Control - Physical Security Controls:

Dubai Government Organization

3.2.1. Enforces appropriate physical access control perimeters for all physical access points to the organization.

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

3.2.3. Controls entry to ICS facility using physical access control devices.

3.2.4. Controls and monitors physical access to the ICS and nearby environment.

3.2.5. Safeguards and enforces adequate protection controls on systems that manage physical access.

3.2.6. Organization reviews logs of physical access on a regular basis.

3.2.7. Deploys mechanism to monitor the movement of employees & non-employees within the organization.

3.2.8. The organization deploys appropriate power backup solutions to ensure continued operation of the ICS environment within the defined secure state of operation.

4. Main Control - External Party Access Control:

Dubai Government Organization

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

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

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

4.4. Authorizes, monitors and controls entering and exiting the ICS facilities or any other public areas and maintains such records.

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 organization's ICS security policy.

5. Main Control - External Party Access Control:

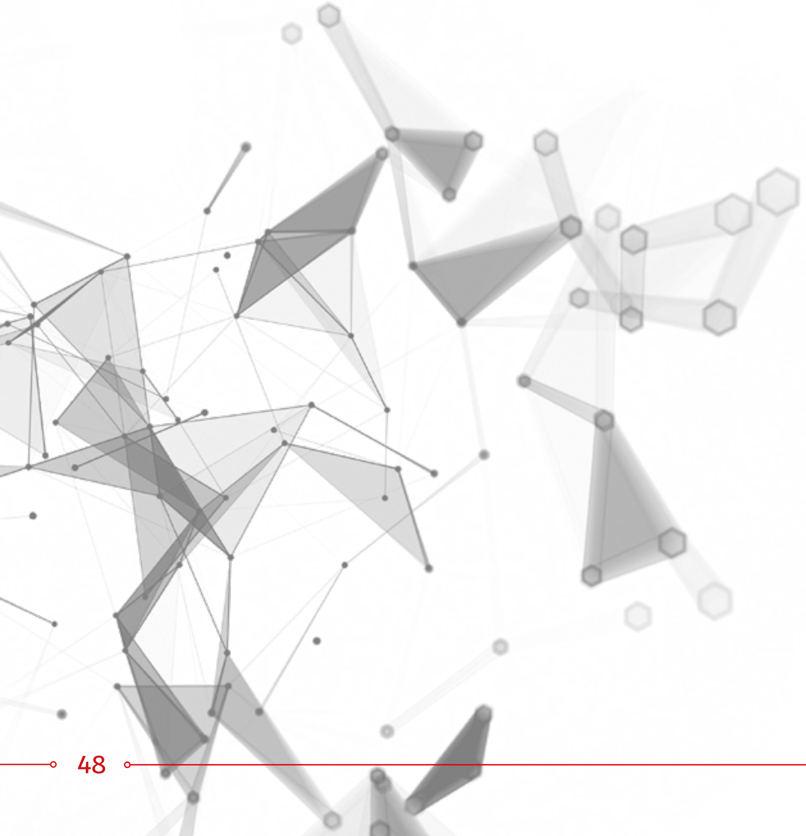
Dubai Government Organization

5.1. Implements audit trails in ICS systems as per requirement.

5.2. Logs, maintains and periodically reviews logical and physical access control lists enabled within the ICS environment.

DOMAIN 6

OPERATION, SYSTEMS AND COMMUNICATION MANAGEMENT



DOMAIN 6 OPERATION, SYSTEMS AND COMMUNICATION MANAGEMENT

OBJECTIVE:

To define controls for mitigation of security risks associated with the daily operations of ICS, Automation processes, maintenance, ICS information storage and data transmission.

1. Main Control - Access Control Management Policy/Procedure:

1.1. Sub Control - Technology and operations Capacity Management:

Dubai Government Organization

1.1.1. Ensures advanced planning for availability of adequate capacity and resources for the Industrial controls systems (including support systems such cybersecurity technologies) and their technology components, in line with applicable regulations.

1.1.2. Conducts an annual projection review of capacity requirements and resources for the Industrial operation systems and their technology components, integrating business requirements, or immediately upon a significant change to existing system.

1.1.3. The automation systems security design and controls should aide in prevention of exhaustion of system resources, especially by less critical and low priority applications or software.

1.1.4. Enables mechanisms for continuously monitoring the software utility of key system resources such that the organization can ensure adherence to control no. 6.1.1.3 in a manner preventing shortage of resources.

1.2. Sub Control - Documentation of Operational Procedures:

Dubai Government Organization

1.2.1. Develops and maintains a complete set of operating procedures documentations of all Industrial operation systems detailing inputs, outputs and dependencies.

1.2.2. Documents and maintains up to date baseline configurations manuals of all ICS operating and engineering systems including an inventory of constituent system components. The baselines should also include cybersecurity configurations.

1.2.3. Only authorized personnel should have access to the baseline configurations. Any changes to the baselines should be logged and reviewed.

1.2.4. Enables adequate approval mechanisms involving necessary stakeholders prior to deploying changes to the ICS Operational procedures.

1.3. Sub control - Change Management:

Dubai Government Organization

1.3.1. Develops, distributes and maintains a documented change management policy that defines the overall change management process employed by the organization for ICS environment, outlining roles and responsibilities.

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.

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.

f) Approved maintenance windows during which the change will be implemented

1.3.4. Incorporates health and safety reviews for all significant changes. Thereby ensuring, continued security and safety of ICS systems.

1.3.5. Whenever applicable, the organization ensures performance of a change impact analysis to derive potential impact to the ICS prior to deployment of changes.

1.3.6. Ensures separation of change responsibilities to employees ensuring no overlap of duties.

1.3.7. Integrates ICS cybersecurity change management procedures with overall ICS change management procedures to enable integration of Cybersecurity within regular operation of the ICS systems and components.

1.3.8. Maintains historical record of all changes being carried out within the ICS, recording necessary information to identify the change, date of change, purpose of change, responsible owner and other necessary information deemed appropriate by the organization.

1.4. Sub Control - Configuration Management:

Dubai Government Organization

1.4.1. Develops and distributes a configuration Management policy enabling the organization to establish baseline configuration requirements, manage configuration changes and define cross-functional responsibilities necessary for the management of ICS Systems/Components configuration.

1.4.2. Implements procedures for management, monitoring and documentation of configuration changes made to the ICS systems such as PLCs, DCS, HMIs, SCADA clients and servers, Operator stations and any other supporting ICS equipment and applications.

1.4.3. Enables access restrictions to ICS system configuration settings and performs periodic reviews to ascertain provision of access to necessary users.

1.4.4. Assessment should be performed to determine the change in cybersecurity risk level due to configuration changes applied on ICS systems.

1.4.5. Ensures changes made to the ICS environment satisfy the cybersecurity requirements to address the risk level and overall provide the same or better degree of protection as the original equipment or configuration.

1.4.6. Establishes and ensures uniform application of minimum-security baseline configuration of ICS systems and components.

1.4.7. Establishes network and security configuration settings for the ICS systems in line with recommendations from corresponding System vendors. organization.

1.4.8. Ensures periodic review and update of ICS security baselines for different ICS components upon identification of new risks, installation of new technology/components or changes to the ICS environment.

1.5. Sub Control - Segregation of Duties:

Dubai Government Organization

1.5.1. Segregates duties and responsibilities as necessary through distributing the tasks for a specific industrial operation / area among multiple users, in a manner to reduce errors, fraud and unauthorized modification or misuse of the organization’s ICS assets.

1.5.2. Enforces restriction of access control to the ICS by implementation of segregation of duties as a part of employee’s job role. Thereby curtailing ICS access on a need-to-know basis and enabling validation by different users prior to deployment of high-risk operations.

1.6. Sub Control - Separation of Operational Facilities:

Dubai Government Organization

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

1.6.2. Allocates secured computing environment for ICS sections performing critical operations.

1.6.3. Ensures that the development tools and compilers are not accessible from ICS operator systems.

1.6.4. Ensures sensitive ICS operational information is not forwarded into the test environment. Thereby restricting access of sensitive plant information only within the organization's ICS.

1.7. Sub Control - ICS Systems Deployment:

Dubai Government Organization

1.7.1. Develop, distribute and maintain a documented policy and procedure for the acquisition, deployment and upgrade of ICS operation systems, addressing the organization's requirements for ensuring security controls implementation and in line with organization's baseline configuration requirements, prior to acceptance or deployment.

1.7.2. Defines and implements acceptance criteria for new ICS systems implementation and upgrades and enforcing documented certification and accreditation process outlining security requirements.

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

2. Main Control - External Party Services Management:

Dubai Government Organization

2.1. Develops, and maintains a documented agreement with the external party service providers that addresses compliance with the organization's ICS security requirements in addition to the organization's ICS security controls.

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.

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

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 organization's policies/procedures.

c) New technology or new vendor to be used.

2.5. Identifies and nominates employees or internal service management teams to ascertain ownership for the management of external party services.

2.6. Incorporates necessary controls for monitoring and reporting of identified security incidents by the third party in agreement contracts to facilitate timely resolution and mitigation of Cybersecurity risks to the ICS.

2.7. Enforces mechanisms to periodically review adherence to contractual statements mentioned in agreements with third parties.

3. Main Control - Protection against Malicious Code:

Dubai Government Organization

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

3.2. Implements documented procedures to deal with malicious code reporting and recovery.

3.3. Conduct regular awareness across the organization on the importance of protecting the organization infrastructure from malicious code attacks.

3.4. Implements organization wide system/software for the malicious code scanning, detection and repairing.

3.5. Anti-malware solutions should be updated on a regular basis with latest signature files.

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

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

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

3.9. Defines the acceptable and unacceptable mobile code technologies.

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

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

3.12. Enforces restrictions on usage of mobile code (like flash & VB scripts, Java, Active x components, Flash, etc.) within the Control System network. Thereby effectively preventing execution of mobile code, restricting transfer of mobile code to ICS and vice versa and monitoring use of mobile code within the operation environment.

3.13. Enables mechanisms to validate the mobile code integrity prior to execution in the ICS environment.

3.14. Enables malicious code protection mechanisms at all entry and exit points of the ICS environment.

3.15. Wherever feasible, the organization ensures central management controls for protection against malicious code.

3.16. Ensures updated malicious code definition files are not directly pushed from the Internet to the ICS systems. Enables manual update mechanism for smaller non-critical ICS systems and centralized mechanisms for updating larger critical ICS systems.

4. Main Control - Network Security:

Dubai Government Organization

4.1. Implements documented process for its ICS network services to govern the interconnections between its network, critical owned business ICS 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.

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.

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.

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

4.5. Implements secure network routing controls.

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 organization or to external network).

4.7. Terminates network connections associated with communication sessions as per the organization defined period of inactivity.

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

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 organization’s change management policy.

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.

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

4.12. Ensures logical separation of IT and ICS networks by means of physical isolation or Firewalls. Also, ensures segmentation of critical ICS networks from other ICS networks to better contain potential cyber threats to the ICS.

4.13. Enables network services to ICS environment without establishing connections to the organization’s IT environment.

4.14. Ensures monitoring and control of communications within ICS zone boundaries to analyse network traffic and ascertain control upon identification of malicious traffic.

4.15. Enables islanding of organization’s ICS communication network upon occurrence of incidents and ensures deployment of fail close mechanisms upon failure of ICS boundary protection systems.

4.16. Enables provisions for operation of ICS in degraded mode upon the occurrence of a DoS (Denial of Service) incident.

4.17. Enables necessary DoS prevention controls to manage ICS communication loads and limit DoS effects within ICS network compartments.

4.18. Provisions capability to restrict/prohibit use of unnecessary services, ports and protocols.

5. Main Control - Information Exchange Management:

5.1. Sub Control - Information Exchange:

Dubai Government Organization

5.1.1. Develops, distributes and maintains documented policy and procedures governing the exchange of ICS information internally in the organization, 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.

5.1.2. Develops and maintains documented ICS information exchange agreements that cover the protection and non-disclosure requirements for the exchange of any government related information between the organization and any external party.

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.

5.1.4. Enforces restrictions on person-to-person communication channels connecting ICS and IT environments.

5.1.5. Implements mechanisms to secure exchanged information from interception, misrouting, modification etc.

5.1.6. Enables mechanisms for detection and protection from malicious code that might be transmitted over electronic media.

5.1.7. Ensures provision of awareness trainings to employees on the secure utility, storage and exchange of information and specifies responsibilities of information users towards safeguarding the confidentiality and integrity of the information.

6. Main Control - Media Handling Management:

Dubai Government Organization

6.1. Develops and distributes a Media Handling policy specific to the ICS environment to prevent unauthorized disclosure, modification or destruction of ICS assets.

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

6.3. Enforces storage of removable media in a secure manner in line with storage instructions provided by the manufacturer.

6.4. Enables documented procedures for the secure and safe disposal of media when no longer required. Thereby safeguarding the confidentiality of critical/ sensitive ICS information.

6.5. Implements labelling/classification of ICS information types to ensure adequate deployment of security controls for corresponding ICS information.

7. Main Control - Monitoring and Logs Management:

Dubai Government Organization

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

7.2. Sets adequate monitoring requirements for all ICS systems/ applications based on criticality of the systems.

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

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

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

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

7.7. Sets an appropriate lifetime for maintaining the logging information, as per the business needs and criticality of information.

7.8. Enables clock synchronization over all information processing systems/

applications with accurate time source. Wherever applicable the organization ensures generating an audit event upon alteration of time source.

7.9. Ensures logging of events for necessary ICS operations and security functions. The logs contain necessary information such as timestamps, source, event ID, type, category etc.

7.10. Wherever feasible, the organization enables centrally managed audit logs compiled from multiple sources across the ICS, enabling comprehensive visibility of the ICS environment.

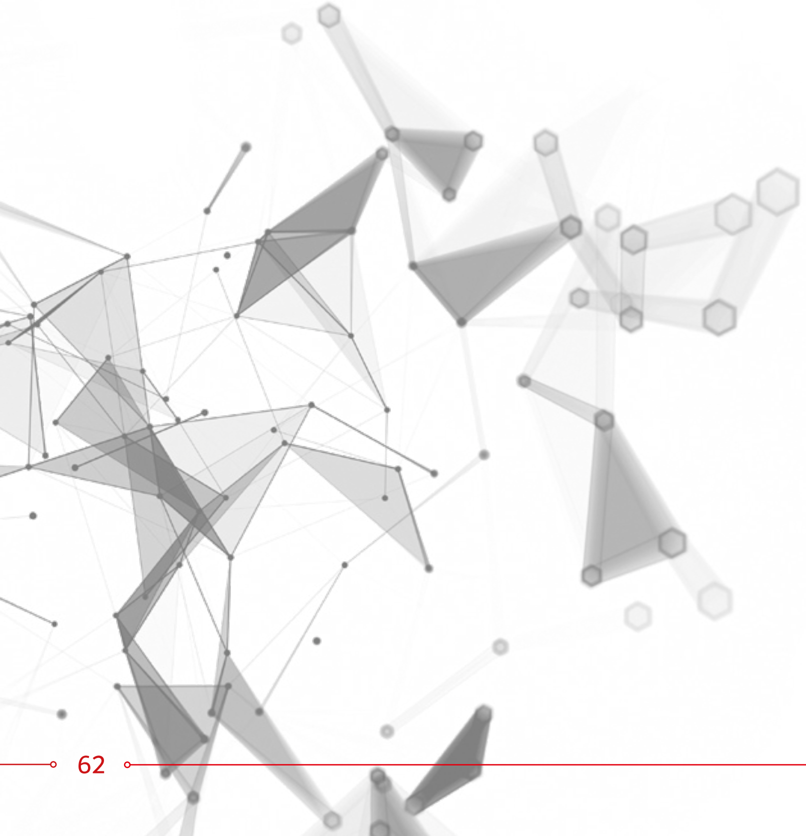
7.11. Provisions storage capacity for the recording of ICS system audit logs based on defined storage requirements calculated considering likelihood of event occurrence.

7.12. Enables mechanisms to protect the integrity of Audit logs from modification, deletion or unauthorized access.

7.13. Ensures provision of audit logs to authorised users only in Read-only formats.

DOMAIN 7

BUSINESS CONTINUITY PLANNING



DOMAIN 7 BUSINESS CONTINUITY PLANNING

OBJECTIVE:

To ensure continuity of business operations upon the occurrence of a service disruption by means of identifying critical functions within the ICS and enabling necessary strategies for developing system redundancies, acquisition of spares and review processes.

1. Main Control – Business Continuity Planning Policy and Procedures:

Dubai Government Organization

1.1. Develops and distributes a Business Continuity Policy and Procedure incorporating employee roles and responsibilities, operational guidelines, necessary actions and mitigation methodologies for ensuring continuity of the organization’s ICS environment.

1.2. Enables mechanisms to conduct periodic reviews and updates to the Business continuity planning framework in line with the business requirements, Changes to ICS systems, processes, current ICS trends and risks.

2. Main Control - Business Impact Analysis:

Dubai Government Organization

2.1. Develops and periodically conducts a business impact analysis for all critical business processes and ICS systems to define and determine the impact of potential operational failures.

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

2.3. Identifies, documents and periodically reviews operational incidents that adversely affect the ICS systems and components.

2.4. Derives probability and impact of identified operational incidents on the ICS security and overall business process of the organization.

3. Main Control - Business Continuity Plan:

Dubai Government Organization

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

3.2. Develops, maintains, periodically tests and reassesses a business continuity plan that covers the following.

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

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

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

3.6. Organization Designs a business continuity process in a manner to reduce the impact of a major disruption on key ICS processes.

3.7. Ensures inclusion of ICS Cybersecurity procedures to recover from a disaster or outage within the organization’s overall Business Continuity plan.

3.8. Ensures adequate coverage of all applicable ICS system entities such as PLCs, DCSs, HMIs, SCADA applications, Operator and Engineering stations, SCADA servers etc. in the Business continuity plan such that designed recovery strategy is comprehensive and applicable.

3.9. Appoints and educates designated personnel for the appropriate execution of the ICS system recovery by means of developing Business continuity procedures.

3.10. Identifies critical business needs associated with the ICS and defines recovery objectives to be incorporated in Business Continuity Plan.

3.11. Develops and assesses a list of potential disruption scenarios applicable to the organization’s ICS environment to support with the designing of recovery procedures.

3.12. Enables approval mechanism for acceptance of designed Business Continuity Plan from appropriate stakeholders within the Organization.

3.13. Enables mechanisms to update the Business Continuity Plan accounting for changes in operational environment, new threats to the ICS operation and changes in business requirements.

3.14. Trains relevant employees on their Business continuity roles and responsibilities. Thereby, enabling a quick and suitable action upon the occurrence of an ICS security incident.

4. Main Control - Disaster Recovery:

Dubai Government Organization

4.1. Identifies the most critical ICS systems and applications in accordance with the risk assessment conducted by the organization.

4.2. Deploys a recovery plan for the identified critical business systems, as the organization’s operations specify.

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

4.4. Exercises and periodically tests the decided recovery plan.

4.5. Establishes a Disaster recovery site based on risk assessment and a business impact analysis to help the entity recover business systems that are critical to operations.

4.6. Assigns Disaster Recovery roles and responsibilities to appropriate employees and ensures provision of necessary training and resources.

4.7. Records and stores necessary ICS information such as: Physical and logical access lists to the ICS, Updated ICS network schema and ICS component configuration information.

5. Main Control - Backup and Storage Strategies:

5.1. Sub Control - Backup and Storage Policy and Procedure:

Dubai Government Organization

5.1.1. Develops, distributes and maintains a 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.).

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

5.1.3. Defines ICS backup restoration speed and frequency requirements. Thereby, enabling backup systems acquisition strategy to support with the organization's recovery objectives.

5.2. Sub Control - Media Library and Resources Protection:

Dubai Government Organization

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

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

5.2.3. 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.

5.2.4. Allocates locations, with adequate security and environmental measures and controls for the storage of the backup media, whether on-site/ off-site, as the organization specifies.

5.2.5. Sets security agreements and security protection controls in case an external party is involved in handling the media library for the organization.

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

5.2.7. Encrypts backups and archives where technically feasible and appropriate.

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

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

5.3. Sub Control - Backup Testing Restoration:

Dubai Government Organization

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

5.3.2. Ensures the restoration and recovery of the ICS to a known secure state of operation after an operational failure or disruption thereby enabling complete system functionality with known security assurance.

5.4. Sub Control - Control System Backup:

Dubai Government Organization

5.4.1. Ensures deployment of mechanisms to conduct backups of user-level and System-level information within the ICS without disruption of regular operations.

5.4.2. Enables automated backup mechanisms for obtaining specified backup information from the ICS on a pre-defined frequency.

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

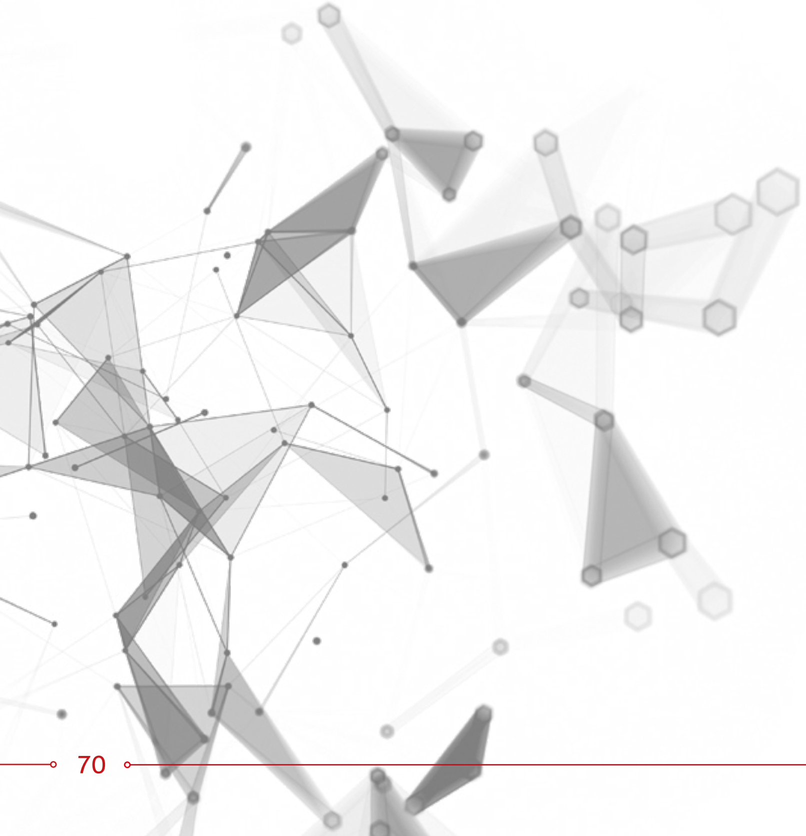
Dubai Government Organization

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

6.2. Reviews and tests defined Business continuity procedures to ensure adequate mitigation of risks within the ICS environment in line with changes in ICS systems, business requirements and current ICS risks.

DOMAIN 8

ICS SYSTEMS ACQUISITION, DEVELOPMENT AND MANAGEMENT



DOMAIN 8 ICS SYSTEMS ACQUISITION, DEVELOPMENT AND MANAGEMENT

OBJECTIVE:

To define controls to ensure that information systems are acquired, developed and managed keeping relevant security aspects into consideration.

1. Main Control - ICS Systems Acquisition, Development and Management:

1.1. Sub Control - ICS Systems Acquisition, Development and Management Policy and Procedure:

Dubai Government Organization

1.1.1. Develops, distributes and maintains a documented policy and procedures for addressing the organization’s requirements for ensuring the security on any in house developed or external party applications regarding the Acquisition, Development and Management of ICS systems, including mobile applications.

1.1.2. Enables mechanisms for periodically reviewing the ICS Systems Acquisition, Development and Management policy and procedures to ensure coverage of current Information security risks, changes within organization's ICS environment and business requirements.

1.2. Sub Control - ICS Application security:

Dubai Government Organization

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.

1.2.2. Defines, distributes and maintains a documented 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.

1.2.3. Ensures ICS applications are enabled with adequate security controls around input data validation such as:

a) Validation of input data to applications such as out of range value checks, missing information check, unauthorized/incorrect data check etc.

b) Review of hard copy data sheets for validating integrity of input information.

c) Identifying select stakeholders for the data input process and ascertaining responsibility for input of data.

1.2.4. Incorporates internal application processing checks for safeguarding against corruption of application information.

1.2.5. Ensures protection of ICS application information integrity by deploying technical controls to enforce security of information at rest and transit such as cryptography.

1.2.6. Ensures ICS applications are enabled with adequate security controls around output data validation such as:

a) Validation checks for ensuring accuracy, completeness and classification of output information.

b) Identifying select stakeholders for validating the data output process.

1.3. Sub Control - ICS system operational requirements:

Dubai Government Organization

1.3.1. Dubai Government Organization.

1.3.2. Enables pre-determined output production upon the failure to operate the organization's ICS environment in normal conditions.

1.3.3. Ensures integrity of monitoring and control sessions between field devices, process network and operator and Engineering stations.

1.3.4. Enforces necessary security controls relating to invalidation of user sessions upon termination/logout of sessions, generation of unique session IDs and random generation session IDs for each session.

2. Main Control - ICS Systems Security Requirements and Specifications:

Dubai Government Organization

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

2.2. Ensures enough coverage of ICS systems and components for application of ICS security such as ICS applications, operating systems, SCADA servers, SCADA systems, PLCs, DCSs, Engineering and Operating stations etc.

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

2.4. Secure coding standards are used for ICS system software and ICS application development.

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

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

2.7. Performs necessary FAT/SAT security tests on ICS components prior to installation and employs measures to perform security tests during regular plant operation in line with business risk and operational constraints.

2.8. Involves necessary control system vendors/system integrators for testing designed security controls.

2.9. Enables application, services and data partitioning for critical functions within the ICS environment. Thereby ensuring operational independence and isolated security.

2.10. Ensures specification of security requirements on contracts/agreements pertaining to installation of ICS systems in accordance with the organization's ICS Cybersecurity framework.

2.11. Wherever deemed appropriate, the organization chooses to acquire security certified ICS products, or the organization enables independent security evaluation of the ICS product prior to Acquisition.

3. Main Control - Secure and Correct Processing of ICS Systems:

Dubai Government Organization

3.1. Conducts testing to validate integrity of data input controls on Industrial Control systems.

3.2. Identifies integrity requirements for processed messages and information in the ICS systems and ensures implementing adequate controls to protect it.

3.3. Integrates validation checks into Industrial Control systems processing to detect any loss of integrity in processed information.

3.4. Conducts testing to validate integrity of data output from Industrial Control systems.

3.5. Adopts transmission security measures, such as cryptography, where feasible, to enable security for ICS information in transit. Thereby, ensuring integrity of transmitted information.

3.6. Ensures integrity of ICS applications and other relevant ICS software by enabling detection, recording, reporting and protection against unauthorized changes.

3.7. Wherever feasible, the organization enables automated notifications to designated users upon detection of anomalous changes to the ICS software.

3.8. Enables validation of syntax and content of any input that affects the operation of the ICS environment directly.

4. Main Control - Securing ICS Systems Files, Source Codes and Data:

Dubai Government Organization

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

4.2. Implements protection controls on the use of testing data.

4.3. Implements access control procedures on ICS systems/application source codes.

4.4. Ensures the Operator stations only process authorized executable code and ensures compilers and command windows are disabled.

4.5. Enables mechanisms to store all previously installed ICS system configurations and enables mechanisms to rollback configurations in case of operational issues.

4.6. Enables adequate security controls for ICS Information systems in test environments such as authorization control for replication of operational information into test environment and purging of operational information post completion of testing.

4.7. Restricts access to program source codes only to authorized personnel.

4.8. Ensures ICS operator stations do not house Program source libraries.

4.9. Enables change control mechanisms for managing changes to the program code such as updating program code and copying program code.

5. Main control - Managing Changes in Software Development:

Dubai Government Organization

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

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

5.3. Implements controls to limit the risk of changes to software packages.

5.4. Implements controls to prevent information leakage in all ICS systems/ application environments.

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

6. Main control - Security Testing:

Dubai Government Organization

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

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

6.3. Identifies current upgrades and updates available for individual ICS assets and the released versions of the updates compatible to the ICS systems on a periodic basis.

6.4. Enables provision of test environment for testing patch updates prior to deployment in the actual operational environment to avoid any unwarranted disruption of systems because of system patches.

6.5. Enables maintenance of a system inventory capturing information relating to ICS system installed versions, authorized versions, effective versions and released versions and ensures mechanisms to update the inventory at periodic intervals.

6.6. Ensures patches are applied for system components within the ICS environment whenever a vulnerability is identified or as communicated by vendors.

7. Main control - Deployment of ICS Systems / Applications:

Dubai Government Organization

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

7.2. Implements security sign off process to confirm the implementation of security controls on all ICS systems/applications prior to deployment.

8. Main Control - Cryptography Controls:

Dubai Government Organization

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.).

8.2. Implements cryptography and key management mechanisms as required by the organization.

8.3. Implements protection and security controls on all cryptographic keys used by the organization in accordance with good industry practices.

8.4. Wherever applicable, the organization ensures adherence to the Dubai PKI requirements within the ICS:

a) Certificate validation by means of validation of the certificate signature.

b) Creation of a certification path to an accepted Certification Authority for validation of certificates.

c) Validation of certificates by verification of a certificate's revocation status.

d) Enforcement of user control on the corresponding private key.

e) Mapping the authenticated identity to a user.

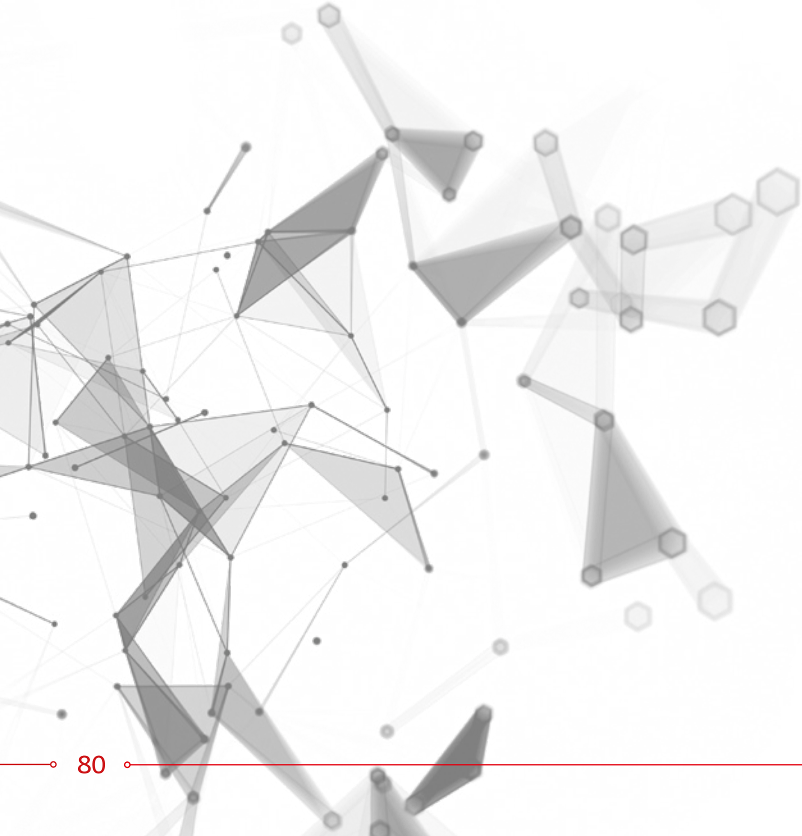
8.5. Enables mechanisms to physically secure the relevant private keys within the ICS environment by means good industry practices.

8.6. Employs mechanisms to record actions taken by a user to define responsibility of the action to the user.

8.7. Deploys Cryptographic encryption mechanisms on the ICS environment after considering impact on system performance and operations.

DOMAIN 9

ENVIRONMENTAL AND PHYSICAL SECURITY



DOMAIN 9 ENVIRONMENTAL AND PHYSICAL SECURITY

OBJECTIVE:

To secure physical premises of the ICS environment to protect ICS assets, process information systems and associated resources from unauthorized access, and physical damage.

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

Dubai Government Organization

1.1. Develops, distributes, and maintains a documented, environmental threats protection policy that addresses the organization’s requirements for placing environmental protection controls.

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

1.3. Ensures the Environmental and Physical protection policy and procedures are periodically reviewed and updated; incorporating changes to the ICS environment, current threats to the ICS and change in business requirements.

2. Main Control - Protection from Environmental Threats:

Dubai Government Organization

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

2.2. Controls humidity and temperature level on ICS rooms, and continuously monitors it.

2.3. Implements fire suppression and detection systems.

2.4. Implements control for monitoring water leakage at the ICS rooms.

2.5. Wherever applicable, Protects ICS systems and components from dust by provisioning a filtered environment.

2.6. Deploys suitable alarming mechanisms to indicate unfavourable environmental conditions to facilitate necessary actions from ICS system users and owners.

3. Main control - Secure Working Areas:

Dubai Government Organization

3.1. Implements adequate physical security mechanisms in control rooms, data centers, and other working areas, based on criticality of such areas within the ICS environment.

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

3.3. Implements security controls over delivery and loading areas.

3.4. Enables appropriate Physical Access limitation mechanisms for Control rooms, Electrical rooms, Server rooms etc. within the ICS to prevent unwarranted users from accessing these critical ICS environments.

3.5. Reviews physical access lists to the ICS environment and ensures appropriate access provision in line with user roles and responsibilities and enables removal and addition of users to the access list.

3.6. Wherever deemed necessary, develops secondary control rooms for ascertaining appropriate operation of ICS if the primary control room becomes inhabitable.

3.7. Enables mechanisms to monitor physical access to the ICS environment to detect, analyse and respond to physical security incidents.

3.8. Maintains physical/digital records about visitors who access the ICS Environment.

4. Main control - Secure Working Areas:

Dubai Government Organization

4.1. Places ICS systems related equipment in secure and protected locations.

4.2. Protects power equipment and cabling of the ICS environment from damages.

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

4.4. Implements maintenance procedures for all ICS systems and components.

4.5. Implements adequate security controls on the disposal or re-use of any equipment.

4.6. Enables provisions to physically track the location and movement of ICS assets.

4.7. Ensures appropriate authorization mechanisms prior to movement of ICS equipment outside the premises.

4.8. Maintains records of personnel with authorized access to designated zones within the ICS environment.

4.9. Enables mechanisms to control ICS environment access to visitors by enabling necessary access control mechanisms such as entry/exit logs, swipe cards, electronic passes etc.

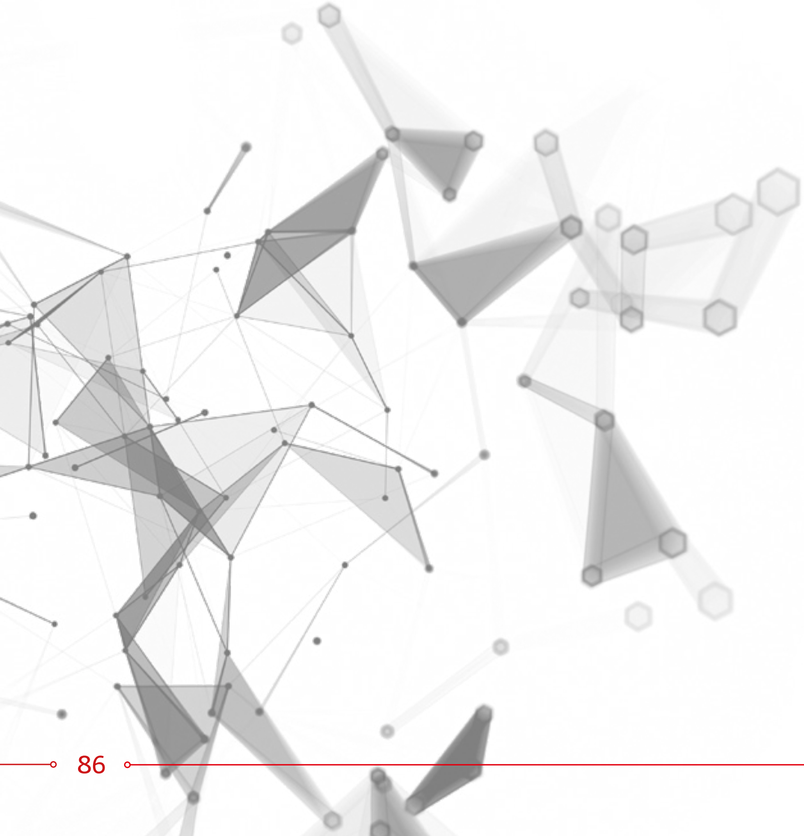
5. Main control - Periodic Testing:

Dubai Government Organization

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

DOMAIN 10

ROLES AND RESPONSIBILITIES OF HUMAN RESOURCES



DOMAIN 10 ROLES AND RESPONSIBILITIES OF HUMAN RESOURCES

OBJECTIVE:

To ensure that all employees, contractors and outsourced employees operating within the ICS environment are aware of their obligations towards ICS cybersecurity and that their roles and responsibilities are defined in relation to securing organization's ICS systems and related information.

1. Main control - Prior to Employment Security Controls:

Dubai Government Organization

1.1. Defines security roles and responsibilities of employees, contractors and outsourced employees in alignment with the organization's ICS Cybersecurity framework.

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

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

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

1.5. Incorporates ICS cybersecurity awareness as part of induction programs of newly hired employees, contractors and outsourced employees.

1.6. Conducts ICS Cybersecurity awareness, learning and training sessions for operators, automation engineers and other personnel working within ICS environment.

2. Main control - During Employment Security Controls:

Dubai Government Organization

2.1. Establishes the requirement for the senior management to be responsible for enforcing compliance of their employees, contractors and outsourced employees to the organization's information security and ICS cybersecurity policies and procedures.

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

2.3. Ensures that all employees, contractors and outsourced employees are provided with information and ICS cybersecurity awareness programs on a regular basis.

2.4. Ensures periodic ICS Cybersecurity awareness and training sessions for relevant employees on a regular basis.

3. Main Control - Termination/Change of Employment Security controls:

Dubai Government Organization

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

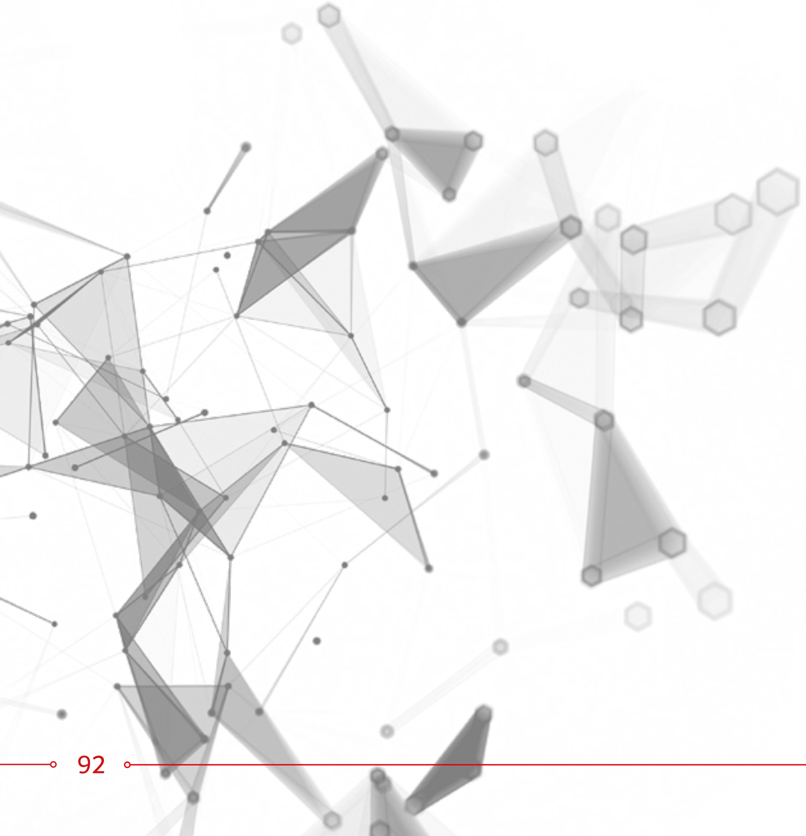
3.2. Communicates termination responsibilities to the terminated employee in relation to confidentiality agreements and employment contracts.

3.3. Implements a process for returning all organization’s assets upon termination of employment.

3.4. Implements a process for revoking or changing access rights and privileges to the ICS environment upon termination or change of employment.

DOMAIN 11

COMPLIANCE AND AUDIT



DOMAIN 11
COMPLIANCE AND AUDIT

OBJECTIVE:

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

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

Dubai Government Organization

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 Centre 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 ICS security.

2. Main Control - Compliance Controls:

Dubai Government Organization

2.1. Identifies the laws or regulations that are applicable to the organization's ICS environment and ensures adherence to the ICS security framework.

2.2. Develops and distributes policies and procedures for conducting periodic security audits with the organization's ICS environment.

2.3. Ensures mechanisms to update the Audit and Compliance policy and procedures to accommodate for changes in ICS risks, ICS technical and process environment and business requirements.

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

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

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

2.7. Ensures validation of security controls deployed during installation of ICS assets for accuracy and ensures adherence to change management controls defined within the ICS Cybersecurity policy by means of reviewing audit trails, approvals etc.

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

Dubai Government Organization

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.

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

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

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.

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

4. Main Control - Compliance with ICS Security Policies and Standards:

Dubai Government Organization

4.1. Conducts periodic reviews to verify compliance of the implemented ICS security policies and procedures.

4.2. Conducts periodic technical reviews on ICS systems to verify compliance with the security controls/standard.

5. Main Control - Audit of ICS Security Controls Implementation:

Dubai Government Organization

5.1. Plans and conducts internal periodic audits to verify and report effectiveness of the implementation of the ICS Security controls.

6. Main Control- Audit of Information Security Regulation Implementation:

Dubai Government Organization

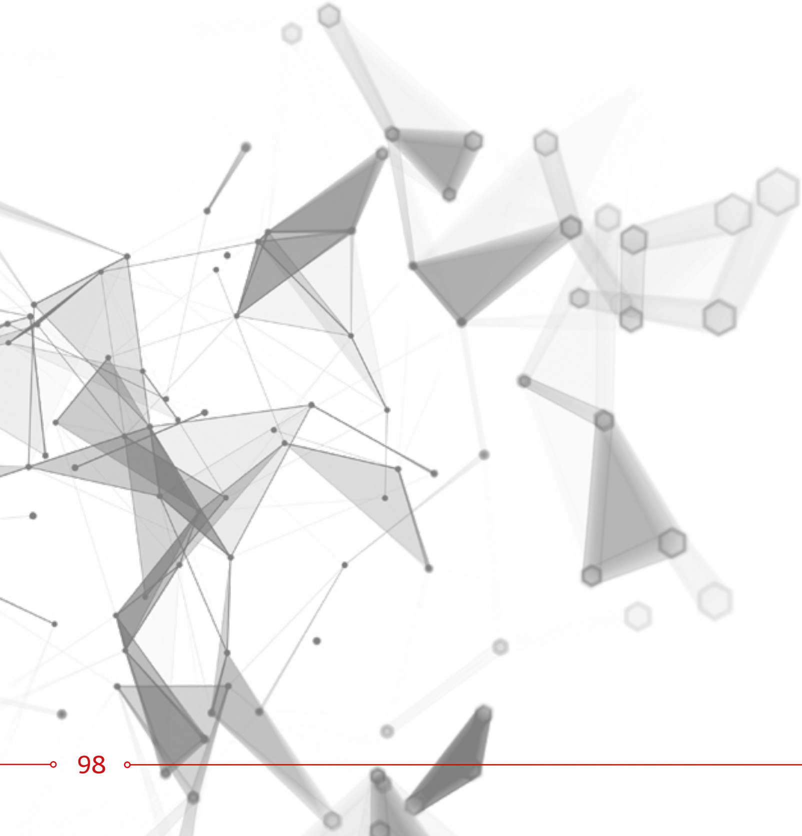
6.1. Develops, distributes and maintains a policy for conducting periodic ICS security audits (risk-based audit) covering governance, operations and assurance aspects of the organization's operations.

6.2. Develops, distributes and maintains a documented procedure, explaining the process for execution, to facilitate the implementation of the ICS security audit policy.

6.3. Plans and conducts internal periodic audits to verify and report effectiveness of the implementation of the ICS Security & applicable standards, in line with the defined policy and procedure.

DOMAIN 12

ICS CYBERSECURITY ASSURANCE AND PERFORMANCE ASSESSMENT



DOMAIN 12 ICS CYBERSECURITY ASSURANCE AND PERFORMANCE ASSESSMENT

OBJECTIVE:

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

- Increase accountability
- Improve ICS Security effectiveness
- Demonstrate compliance
- Provide quantifiable inputs for resource allocation decisions.

1. Main Control - ICS Security Key Performance Indicators:

Dubai Government Organization

1.1. Develops, selects and implements a set of ICS Security Key Performance Indicators (KPIs) that are:

a) In support of the government organization strategic and operational planning processes to secure the organization's mission.

b) Integrated into the annual reporting of effectiveness of the government organization's ICS security controls.

c) Defined to assist in monitoring compliance with the ICS Cybersecurity Regulation.

d) Reviewed regularly and used to support policy, resources allocation, budget decisions, and as an assessment of ICS 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 organization's stakeholders, such as ICS 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 ICS security processes.

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

1.3. Approves the organization's ICS Security measurements and Key Performance Indicators (KPIs) by the higher management of the organization.

1.4. Conducts periodic reviews on the results of ICS security measurements to ensure continual improvement of the ICS Cybersecurity program within the organization.

1.5. Records actions and events that could have an impact on the effectiveness or performance of the ICS Cybersecurity standard.

2. Main Control - ICS Cybersecurity Dashboard:

Dubai Government Organization

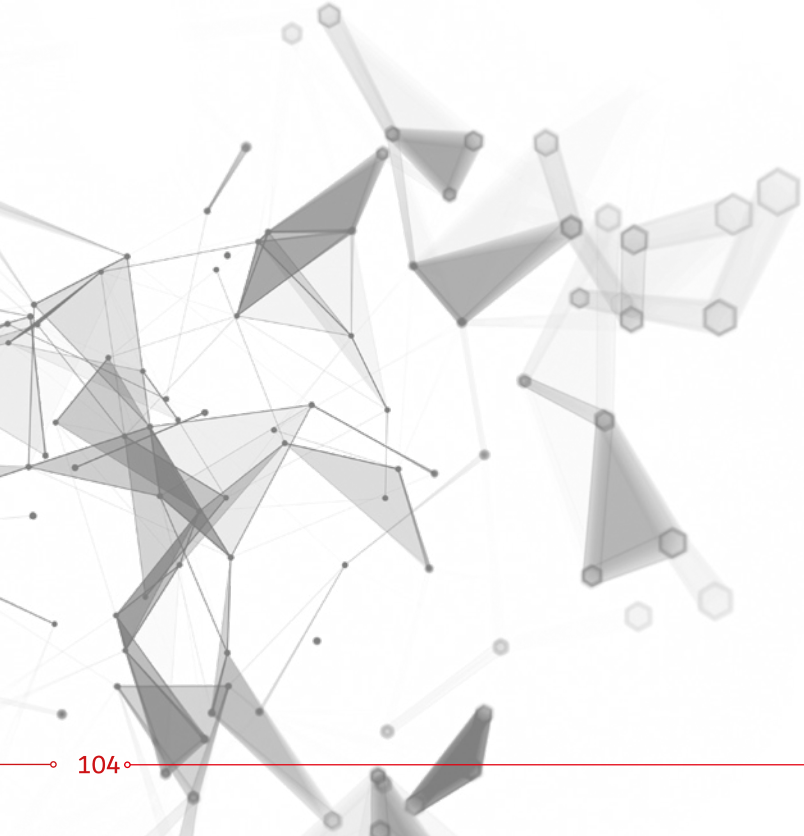
2.1. Implements, as necessary, an integrated dashboard (or incorporates into an existing organization Performance Measurement tool) for combining all measured ICS Cybersecurity KPIs to be reviewed and monitored in a periodic manner, by the senior management and the responsible stakeholders, to ease the decision-making process, and facilitate the overall planning for the ICS Cybersecurity program.

DUBAI ELECTRONIC SECURITY CENTER

مركز دبي للأمن الإلكتروني

DOMAIN 13

CLOUD SECURITY



DOMAIN 13
CLOUD SECURITY

OBJECTIVE:

To set controls for mitigating risks associated with cloud computing and usage of cloud services within the ICS environment.

1. Main Control - Cloud Security Policy / Procedure:

Dubai Government Organization

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

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

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

2. Sub Control - Logical Access Control:

2.1. Sub Control - Data Location:

Dubai Government Organization

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.

2.2. Sub Control - Data Classification and Handling:

Dubai Government Organization

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).

2.3. Sub Control - Architecture and Deployment Model:

Dubai Government Organization

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

2.4. Sub Control - Service Agreements:

Dubai Government Organization

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

2.4.2. Develops and maintains a documented agreement with Cloud Service Provider (CSP) addressing the following ICS security requirements as a minimum:

a) ICS security risks and mitigation

b) Data protection and storage

c) ICS security incidents handling

d) Change, Recovery and Restoration.

2.5. Sub Control - Data Portability and Continuity:

Dubai Government Organization

2.5.1. Ensures that Cloud Service Provider (CSP) has the adequate measures and processes to support data portability whenever the organization decides to move its data.

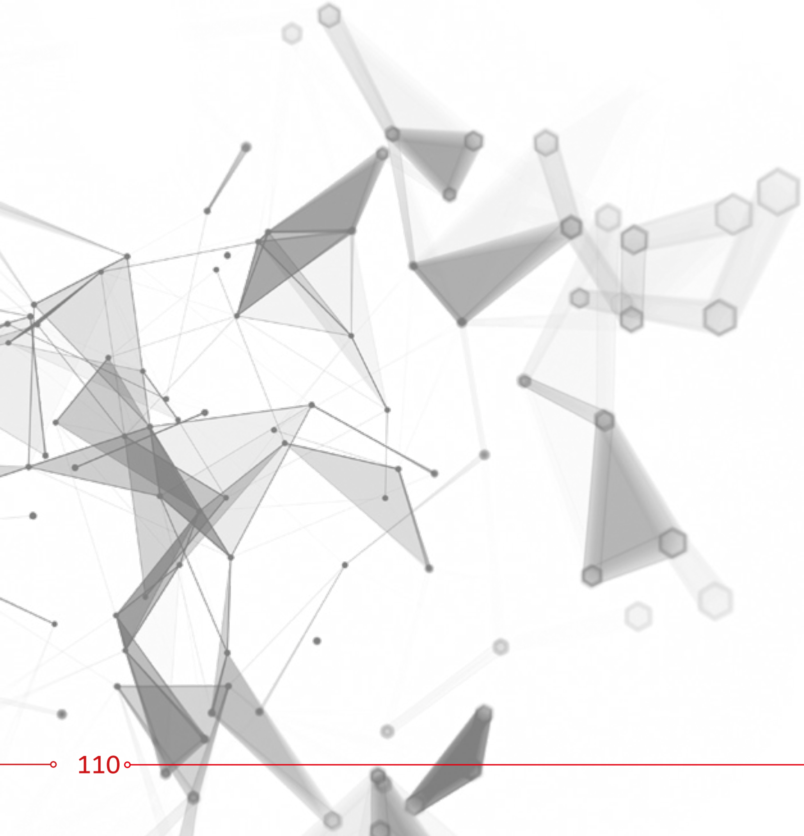
2.5.2. Ensures cloud security controls are implemented by Cloud Service Provider (CSP), addressing organization's requirements for periodic testing of the continuity and disaster recovery plans and communicating the results to organization.

2.6. Sub Control - Compliance and Monitoring:

Dubai Government Organization

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

GLOSSARY



GLOSSARY

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.

Asset Owner

Person or department responsible for the entire lifecycle of the asset. Responsible for budget, approvals and has key decision-making role for that asset.

Asset Custodian

Person or department with delegated responsibility for protecting an asset.

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 (fingerprint).

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 an outcome than any other technique, method, process, etc. when applied to a 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. 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 preset 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 this 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.

Denial of Service (DoS)

An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.

Disaster

Disaster is the tragedy of a natural or human-made hazard (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.

Industrial Control Systems (ICS)

Industrial Control System (ICS) is a collective term used to describe different types of control systems and associated instrumentation, which include devices, systems, networks and controls used to operate and/or automate industrial processes.

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 has any property rights to the asset. Routine tasks may be delegated, e.g. to a custodian looking after the asset daily, 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 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.

Operational Technology (OT)

Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Physical Access Control

Physical access controls monitor and control the environment of the workplace 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 workplace 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 behavior 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) 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 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 analysing 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.

Software Development Life Cycle (SDLC)

Software Development Life Cycle (SDLC) is a framework defining tasks performed in each step of the software development process.

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

Virtual LAN (VLAN)

A VLAN is a custom network which enables groups of devices from multiple networks (both wired and wireless) to be combined into a single logical network.

Vulnerability

Vulnerability is weakness in an asset that can be exploited