w

Riayati

Information and Cyber Security Standard

Document ID: RYT-PGM-POL-002

Date: 25-Oct-2020 (v1.0)

Document History

Version No.	Date Change Approved	Description of Changes	Impacted Supporting Document(s)	Supporting Document Change / Version No.	Authors
0.1	25-Oct-2020	Initial Document	NA	NA	**MOHAP**
1.0	25-Oct-2020	Reviewed and Approved changes and baselined Version	NA	NA	**MOHAP**

Table 1 Document Version History

Document Reviewer(s)	Signature	Date
MOHAP		25-Oct-2020

Table 2 Document Review Grid

Document Approver(s)	Signature	Date
MOHAP		25-Oct-2020

Table 3 Document Approver Grid

After the approvers accept this document, the approved version becomes the baseline. All changes to the baseline version will need to be approved by approvers mentioned above.

1. Table of Contents

2. BACKGROUND

The adoption of Electronic Communication, Information Technology and the increasing reliance of enterprises on technology has been observed within the Public and Private Healthcare sectors across the globe. UAE has also stepped up to improve efficiency, productivity and agility of its Health Care infrastructure to enhance collaboration and improve public trust in Government Healthcare Services.

Electronic services play a crucial role in the improvement of Quality of Healthcare services and the living standards of the Citizens and Residents of Northern Emirates. Therefore, the Ministry of Health and Prevention (MOHAP) has been committed to the further development of the IT Infrastructure, cyber posture and improved electronic communication to support the vision of Leadership of UAE to provide world-class healthcare services.

With the rapid expansion and development of Electronic Services and technology adoption within the healthcare industry, the consequent ever-evolving Cyber Threat Landscape poses challenges to the crucial electronic services. These may include the range of threats such as “Hacktivism, Organised Cybercrimes, State-Backed Actors” to sabotage the crucial Government Services of the Country or pose potential harm to the national security by compromising critical assets.

Keeping in mind the cyber threats to technology landscape, MOHAP has developed a comprehensive Information Cybersecurity Standard or its Riayati Program refers to as “Riayati Information and Cybersecurity Standard” (Riayati ICS). The purpose of this standard is to standardize security controls across the participating entities and stakeholders to mitigate potential cyber threats. All the participating healthcare entities should make it a priority to implement all relevant controls mentioned in this standard to secure the critical elements (information and assets) of communication from cyber threats.

It is hoped that proper implementation and compliance of this standard will increase service reliability and public trust in Government Healthcare services in the Northern Emirates.

3. INTRODUCTION

3.1. Overview

The Ministry of Health and Prevention (MOHAP) of UAE understands the regulatory requirements of the healthcare sector. Therefore, it has developed its Riayati Information and Cybersecurity Standard (ICS) that focuses on the critical requirements and procedures of security prospect of Healthcare Sector. The standard is designed for all participating healthcare entities, and other stakeholders to comply with security best practices while sharing the health data using the Riayati Health Information Exchange.

This standard is based on the requirements of MOHAP and the Healthcare industry and is aligned with internationally recognized Cybersecurity Standards, Frameworks, and Best Practices.

3.2. Purpose

The purpose of the Riayati ICS is to provide security controls required to protect information services and assets associated with Riayati Program. It will also help to elevate the information security compliance of all supporting services within the healthcare facilities using Riayati platform.

As Protected Health Information (PHI) is considered the most confidential information, it is essential to provide the highest level of protection and safeguards around it to uphold the public trust in the Healthcare services.

The Riayati ICS mandates security safeguard requirements to:

- Ensure Confidentiality and maintain the privacy of PHI (Protected Health Information) and PII (Personally Identifiable Information).
- Protect the integrity/accuracy and quality of healthcare data to ensure patient safety.
- PII and PHI information remains unaltered and valid through its life cycle to be auditable.
- Ensure the availability of critical information to the right resources at the right time, to; support effective and organized delivery of care, and to prepare and predict future demands & trends.
- Ensure that the healthcare facility meets unique demands to remain operational in the face of natural disasters, system failures, and denial-of-service attacks.

3.3. Approach

The substantial reliance on information systems demands the healthcare facilities to enhance their security posture to safeguard against the ever-growing cyber threats to information systems, critical business assets, and highly protected PHI.

High demand for security compliance can be achieved through a risk-based approach. The Riayati ICS provides comprehensive risk management process to build a stable security framework by providing guidelines to identify, assess, mitigate, and monitor risks and threats to get prepared to reduce the adverse impact and to recover from any cyber threats.

3.4. Standard Document Structure

This standard document is organized into three major sections.

1. **Section 1**: Focuses on the introduction and governance aspect of the standard, which includes:
   - Scope and Applicability
   - Assurance Lifecycle
   - Risk Management Lifecycle
   - Adoption and Compliance
   - Stakeholders and Responsibilities
   - Key Considerations
2. **Section 2**: Explains the ten security domains, security controls developed by MOHAP, criteria, and control types with references.

3. **Section 3:** Summarises the standard with appendices, references, and controls mapping tables.

4. SECTION – 1

This section will focus on the introduction and governance aspect of the standard which includes

- Scope and Applicability
- Assurance Lifecycle
- Risk Management Lifecycle
- Adoption and Compliance
- Stakeholders and Responsibilities
- Key Considerations

4.1. Scope & Applicability

4.1.1. Scope

The Riayati Information and Cyber Security Standard developed by MOHAP provides the Management with Strategic and Technical controls of Cyber Security for Healthcare facilities to establish, implement, maintain and improve Cyber Assurance continuously.

This standard is mandated by MOHAP to be complied with, by any Healthcare facilities managing, processing, storing or transmitting the health care information using Riayati Health Information Exchange Services.

4.1.2. Applicability

The Riayati ICS Standard applies to all the MOHAP regulated health care entities and services. It includes all healthcare professionals and supporting staff associated with the participating healthcare facilities and will have access to Protected Health Information. Therefore, it is mandatory pre-requisite for all participating healthcare facilities to implement relevant security protocols mentioned in this standard to get privileged access to Riayati Platform.

The implementation mandate of this standard is defined and required by MOHAP. The implementation of Scope of Applicability (SOA) of security controls is the responsibility of the participating healthcare entities.

4.1.3. Benefits

Ensuring compliance with this standard will demonstrate a commitment by the participating healthcare facilities to upholding MOHAP’s strategic objectives in the UAE Healthcare sector. It also improves the cybersecurity posture of their organization and enhances the security of the Protected Health Information being processed through the entity’s information systems.

The implementation of the Riayati ICS standard will bring the following benefits to the healthcare entities:

- Ensure compliance with international standards.
- Helps reduce operational costs by providing risk treatment and business continuity guidelines.
- Ensure customers’ trust by reducing the likelihood of threats, breaches, violations, and, leakage of information.
- Improvement in the overall security posture of the organization as the standard covers not only the technology part but also includes guidelines for various other business functions, i.e. human resources, physical security, environmental safety etc.

4.1.4. Types of Healthcare Facilities

The Ministry of Health and Prevention (MOHAP) has defined the standard for healthcare facility types based on maturity, risk appetite, and complexity levels as follows:

Facility Type	Description
Large Hospitals or Medical Facilities, Insurance Payers	Hospitals or Medical facilities with a bed capacity of 21 and above. Insurance Payers
Small Hospitals or Medical Facilities	Hospitals or Medical facilities with a bed capacity of up to 20 beds
Medical Centres, Clinics, Pharmacies	Day-care Facilities, Dialysis Centres, Rehabilitation Centres, Diagnostic Centres, Primary Healthcare Centres, Mobile Healthcare Units, Pharmacies
Cloud EMR Vendors	EMR Technology Providers

4.2. Assurance Life Cycle

The Riayati ICS follows a life-cycle approach to establish information assurance which includes various techniques for continuous improvement and enhancement of security posture based on best practices and well-defined activities:

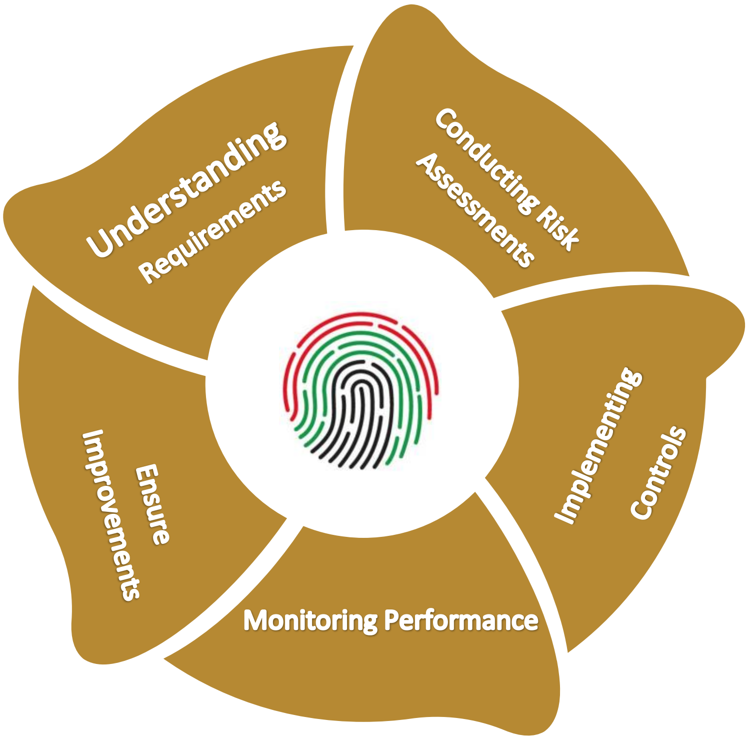
Understanding the healthcare facility's information and cybersecurity requirements to establish a cybersecurity program based on business objectives.

Conducting risk assessments, identifying appropriate risk treatment actions, and selecting cybersecurity controls to manage the risks.

Implementing security controls to manage cybersecurity risks in the context of the healthcare facility and the overall healthcare sector's cybersecurity risks.

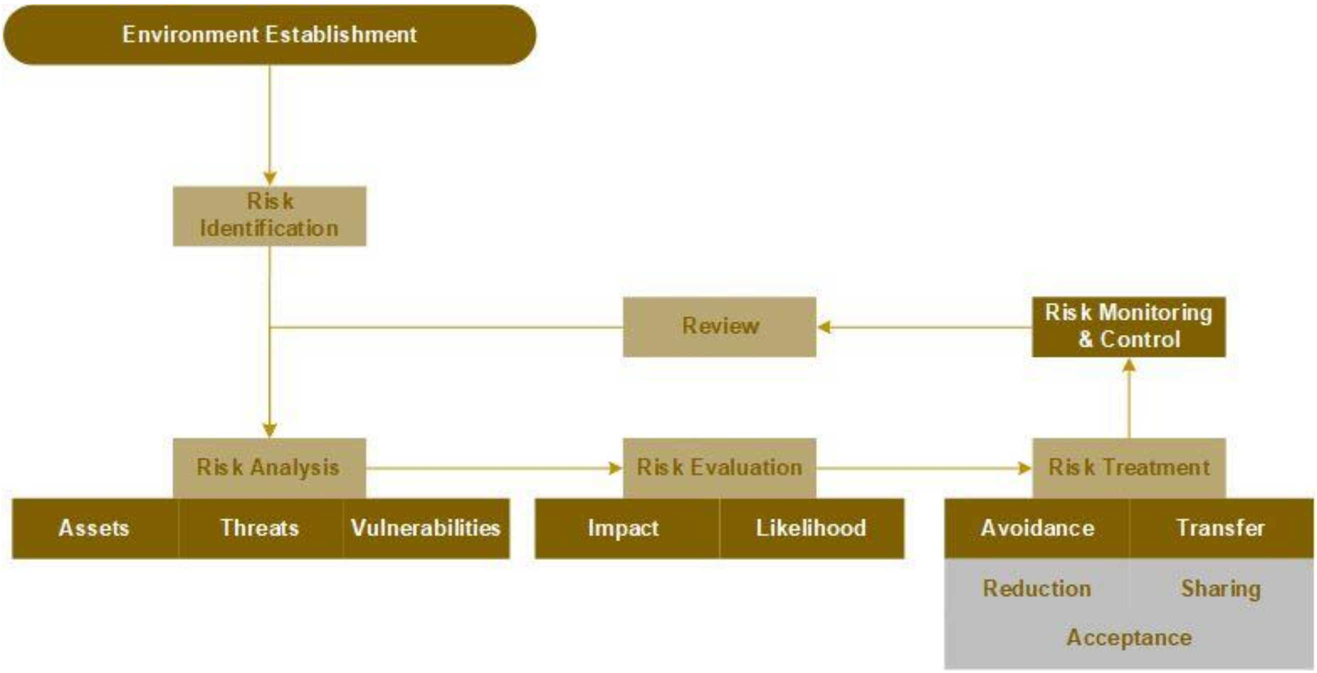
Monitoring the performance and effectiveness of implemented cybersecurity processes and controls.

Ensuring continuous improvements based on business requirements and MOHAP objectives.



4.3. Risk-Based Approach

This approach provides entities with a pragmatic approach to identify vulnerabilities that could be exposed to become threats and have an adverse impact on business functions. This standard put great emphasis on establishing a risk management lifecycle and provides a comprehensive guideline. A Risk Management Lifecycle is based on various phases. It consists of eight key phases, as illustrated below.



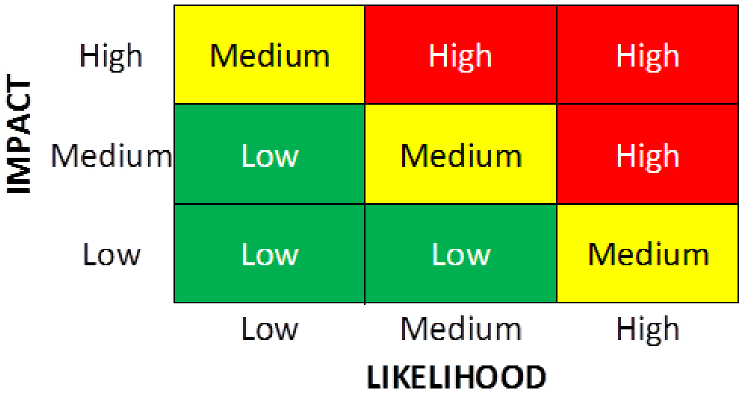
The risk management process is initiated by defining scope, establishing context and parameters of the business functions that are exposed to risks. It is developed further in line with the risk appetite of the organization based on critical security features, i.e. confidentiality, integrity, availability, non-repudiation, accountability, audits, etc.

4.4. Risk Identification

The risk identification phase includes the scope definition and parameter setting of critical business operations and potential risks on the business function, and assets. The objective is to prepare a list of critical business functions and assets that are exposed to potential threats and vulnerabilities based on the cybersecurity requirements of a healthcare entity.

4.5. Risk Analysis & Risk Evaluation

This phase involves the mapping of all the assets, threats and vulnerabilities against the impact and likelihood of occurrence. Upon successful mapping of assets against threats, the immediate step is to assess the risk score through risk evaluation technique. Risk evaluation involves consideration of risk impact in terms of consequences of a loss of confidentiality, integrity, and availability of crucial Protected Health Information (PHI) and the likelihood of occurrence of any exploitation. The output of this process is a risk score. The higher the score, the substantial impact it will make on the asset/business function. The below risk matrix shows the scoring criteria used in the risk analysis and assessment technique.



IMPACT	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
			LIKELIHOOD	

4.6. Risk Treatment

This phase includes the treatment of risk. The risk can be treated through various techniques based on the risk appetite, and operational requirements of the entity.

The following techniques are generally used to treat risk:

- Risk Avoidance: Avoiding the activity or condition that causes the risk.
- Risk Transfer: Transferring the risk to another party.
- Risk Reduction: Reducing the risk by applying security controls.
- Risk Acceptance: Accepting the risk based on the entity's risk acceptance criteria.
- Risk Sharing: Sharing the risk with other parties or individuals.

4.7. Risk Monitoring And Review

Risk management is a non-stop process that adapts and changes over time with any change in business function or process. Therefore, monitoring is a critical phase to ensure the stability of risk management as well as any improvements required to it. This phase involves audits, and surveillance of implemented controls to verify their effectiveness to overall business objective.

During the risk management process, it is crucial to communicate and consult risks with key stakeholders during all stages of the life cycle. Therefore, effective external and internal communication and consultation with relevant stakeholders ensure that everyone understands the severity and ensures accountability to make decisions and take appropriate actions.

4.8. Adoption & Compliance

4.8.1. Controls Types

The security controls included in Riayati ICS are benchmarked against typical healthcare risk register to provide risk treatment profile. It provides convenience in implementing relevant controls against each category. Riayati ICS has classified the controls types into three major areas as below:

- **Strategic Controls**: Controls designed for long-term commitments and overall aims of the healthcare entity's cybersecurity practices.
- **Management Controls**: Controls are designed to make sure that policies are written and reviewed in line with the overall direction.
- **Technical Controls**: Controls are designed to prevent the exploitation of technical vulnerabilities and apply safeguards to protect assets.

4.8.2. Controls Categories

The Riayati ICS mandates minimum requirements of control essential to secure healthcare information and processing facilities. The specified controls are classified into three different categories, applicable to entities based on their risk environment, the type of healthcare information being processed, and the maturity level of the organization.

Controls Category	Definition	Alias
Basic	Controls outlined in this category are the absolute minimum requirement of Information Security and shall be considered the highest priority for compliance. These controls shall protect Information assets from critical threats and shall be considered as a foundation to build on assurance capabilities.	P1
Foundational	Controls outlined in this category are high priority controls to enhance the security posture of healthcare entities. These controls shall protect information assets from a wide range of threats, inclusive of critical and high impact threats, based on the value of information assets owned, managed and handled by the participating healthcare entities. These controls implementation complements in redefining/improving the organization's risk environment.	P2
Organizational	All controls outlined in this category are essential controls, based on an entity status, and shall enhance the security posture of the organization. These controls shall protect information assets from a wide range of threats, inclusive of critical and high impact threats, based on the value of information assets owned, managed, and handled by the participating healthcare entities. These controls implementation elevates the healthcare entity's maturity level and complements the improvement of internal processes and risk environment.	P3

All healthcare entities must comply with the "Basic" level security controls. For any non-compliance to specific necessary control(s), there should be a valid business justification and should be approved by the MOHAP to gain access to Riayati platform.

Control categories are based on the continuous improvement aspect of the Information Security life cycle; this ensures that security capabilities are continuously adapted and evolved in line with changing environment and maturity level.

4.8.3. Healthcare Facilities Classification

MOHAP has defined the facility types matrix based on the complexity levels. The applicability of controls is set to achieve maturity levels according to the risk appetite and entity size.

Facility Type	Description	Controls Applicability	Alias
Large Hospital, Medical Facilities, and Insurance Payers	Hospitals or Medical facilities with a bed capacity of 21 and above.	Basic + Foundational + Organizational	F1
Small Hospital or Medical Facilities	Hospitals or Medical facilities capacity of up to 20 beds	Basic + Foundational	F2
Cloud EMR Vendors	EMR Technology Services Providers	Basic + Foundational + Organizational	F3
Medical Centres, Clinics	Daycare Facility, Dialysis Centres, Rehabilitation Centres, Diagnostic Centres, Primary Healthcare, Mobile Healthcare Units, Drug Stores and Medical Stores	As Defined in Annex	F4

4.8.4. Participant Compliance

The Riayati ICS Standard includes all relevant controls to cover a range of information security domains. Each domain area includes various security best practices and security controls that Healthcare Entity must consider for implementation in a phased manner, based on its risk level and resource availability.

The implementation of these Information Security controls criteria shall be monitored periodically by MOHAP to ensure that they are appropriately implemented, maintained and that associated responsibilities, deliverables and timelines are documented and reported.

Any policy established in support of the implementation of this standard shall have:

- Statement of management commitment
- Purpose of the policy
- Objective of the policy
- Scope of the policy

All the healthcare entities must establish reliable metrics and measurements to identify the state and effectiveness of compliance with required controls. It should produce comparable results through timelines and for any non-compliance, it should be recorded in the entity’s risk register and ensure it is addressed under acceptable criteria defined through this Riayati ICS by MOHAP.

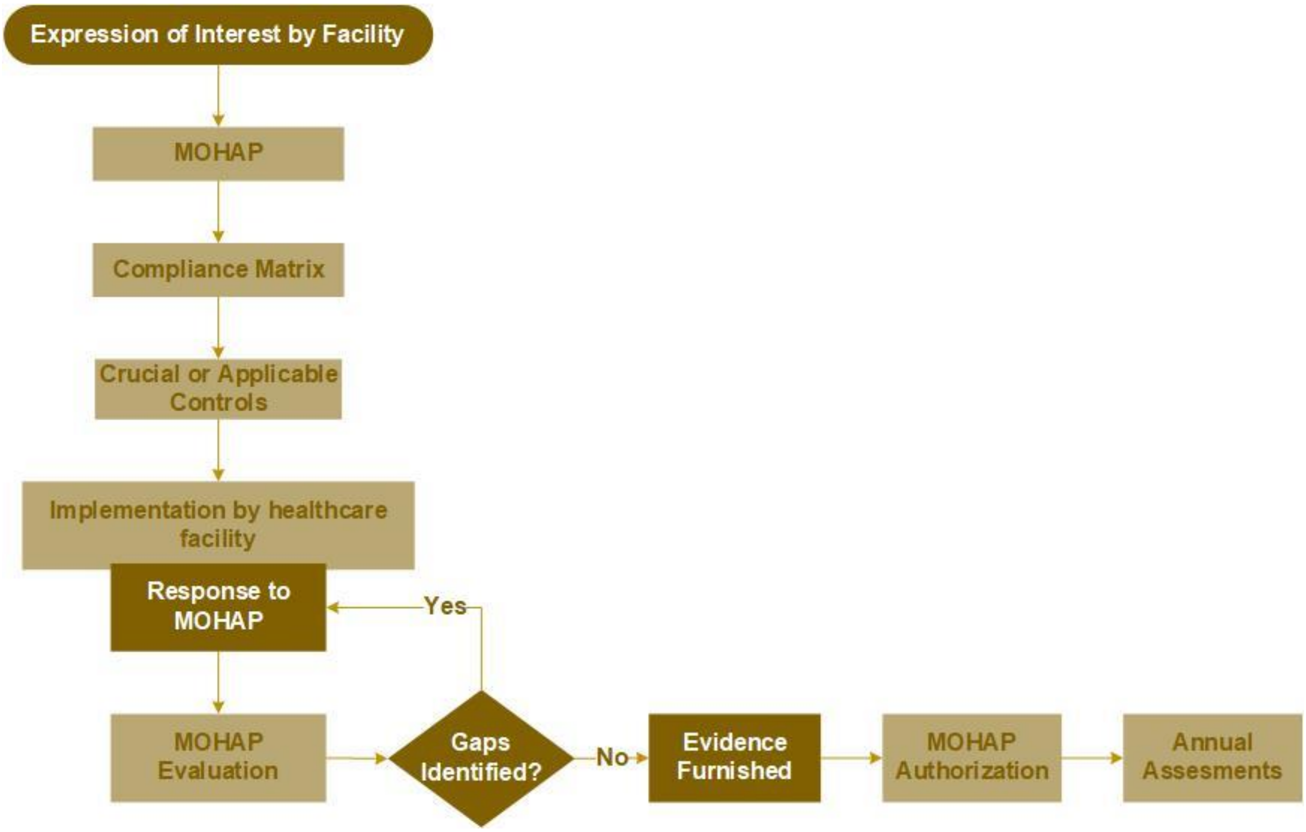
4.8.5. Riayati Onboarding

Riayati ICS requires a certain minimum level of compliance with the security controls as a pre-requisite to onboard any healthcare entity onto the Riayati HIE. The pre-requisite requirements are divided into various phases, and the participating entity must comply with the “Basic Controls Category” requirements within specified timelines before getting onboard.

The timelines may differ for each entity considering the risk environment; however, it is expected that the participating entities comply with a set of security controls provided by MOHAP’s Compliance Matrix within eight weeks of sharing an expression of interest followed by the “Security Assessment” by MOHAP.

MOHAP will evaluate the implementation of the security controls and make necessary decisions of (Approval or Rejection) to proceed further with the onboarding to Riayati Platform. Also, the healthcare entity should consider achieving the maturity levels of the Riayati ICS program based on the entity size and the controls applicability criteria set forth by the MOHAP. The ideal timeline is six months.

MOHAP reserves the right to perform necessary security assessment before providing an authorization of connectivity to ensure the security compliance of the healthcare entity to fulfil the eligibility criteria of onboarding. The flowchart below illustrates the onboarding process.



4.8.6. Assessments & Audits

The healthcare entity shall develop and conduct a formal audit and technical assessments on its information system and application environment periodically (ideally annually) to validate and verify compliance with the provisions of this standard.

The outcome of audits and assessments shall be preserved with the highest level of access protection and secure storage facilities. Tools used for audits and assessments shall be protected from unauthorized access and usage to ensure critical audit and assessment information are secure, not altered or misused.

4.9. Stakeholder's Responsibilities

As the MOHAP, UAE is committed toward their strategic objectives of Riayati Program by designing and implementing security regulation for participating entities for the Riayati program. Similarly, it expects a commitment from participating entities to demonstrate due diligence towards compliance by addressing the information and cybersecurity risks in their environment and investing time and resources to mitigate the risks and maintain a secure and trusted environment and practices.

Therefore, all the participating stakeholders of Riayati programs have specific responsibilities towards their commitments. to implement, improve, and maintain the security of the Riayati Objectives, services, systems, and Information. The responsibilities are listed in the sub-sections below:

4.9.1. Ministry of Health and Prevention

The MOHAP holds the following critical responsibilities to achieve its strategic goals set towards Riayati Program:

- Establish and Maintain the Riayati Information and Cyber Security Standard.
- Enforce the Riayati ICS Standard for UAE National Healthcare Sector covering all aspects, entities, EMR Operators, and other stakeholders.
- Develop an ongoing process to improvise and improve Riayati ICS standard based on industry best practices and learning from industry trends.
- Provide technical assistance, training, support, and possible resources to participating entities to implement the standard.
- Develop processes to conduct periodic assessments of healthcare entities participating in Riayati Program to review their compliance and risk status to ensure compliance goals.
- Provide the participating assistance with communicating with relevant authorities to escalate and report risks, incidents.

4.9.2. Participating Healthcare Entity

The participating healthcare entities hold key responsibilities to achieve MOHAP's objectives towards Riayati Program and Cyber Security as a whole. The healthcare entities responsibilities are listed below:

- Healthcare Entity's Management Responsibilities:
    - Fund and Manage implementation of Riayati ICS standard.
    - Holds accountability for the implementation of the Riayati ICS standard.
    - Supervise information security programs, plans, strategies, initiatives, and policies.

  - Define the Risks treatment processes internally to treat the risks exposed to the Healthcare entity, PHI, or Riayati Program.
- Healthcare Entity Information Security Stakeholders Responsibilities:
  - Provide the Healthcare Entity's internal coordination to implement and maintain the objectives of the Riayati ICS standard.
  - Monitor the risks and report to the Healthcare Management and raise management awareness towards the potential risks.
  - Provide security assurance and risk-based approach in the design, implementation, development, and maintenance of new or any existing information systems and business processes.
- Healthcare Entity's end users' responsibilities:
  - Adhere and comply with the Riayati ICS policies, procedures, and demands.
  - Escalate any non-compliance activity to the relevant designated authority.
  - Assist in improving the overall security posture of the organization by providing valuable feedback and suggestions related to process improvement.

4.10. Key Considerations

The Ministry of Health and Prevention, UAE encourages the participating healthcare entities to define success criteria and critical factors towards the success of the Riayati program. The "Key Considerations towards Success" for the Riayati Program are guided as below:

Provide Awareness within the participating healthcare entity through training and educational workshops. Communicate the information and cybersecurity objective to the leadership, management, employees, and any other stakeholders.

Establish a risk-based information and cybersecurity framework to identify the risk and put applicable information and cybersecurity controls based on expectations and priorities.

Adopt a tailored approach and framework to establish, implement, maintain, and continuously improve cybersecurity posture while considering the risk environment in-line with business and industry requirements.

Develop an understanding to achieve appropriate compliance levels of Riayati ICS to demonstrate the commitment towards MOHAP's objectives.

Implement a measurement system to track compliance, evaluate the performance of the risk-based security framework, and provide feedback/suggestions for the improvement of the Riayati ICS.

Escalate the critical non-compliance cybersecurity information to the MOHAP and relevant authorities to build an intelligent knowledge base for the improvement of the risk landscape of the healthcare sector.

Participate and contribute to communicating best practices with MOHAP to improve the cybersecurity framework of the Riayati Program.

Ensure visible support and commitment from all levels of management.

Provide adequate funding for all Information Assurance activities.

5. SECTION – 2

This section details the different Security Domains, Security controls developed by the Ministry of Health and Prevention, criteria, and controls types with references.

i. Human Resources Security
ii. Asset Management
iii. Physical and Environmental Security
iv. Access Control Management
v. Operations Management
vi. Communications and Application Security Management
vii. Healthcare Information Security
viii. Third Parties and Supply Chain Management
ix. Security Incident Management
x. Information Systems Continuity Management

5.1. Human Resources Security

For any organization's security, Human resources are considered as the weakest security link in the age of digital transformation, mobile business, remote workforces, and interconnectivity. The proactive cybersecurity measures taken by the organization can safeguard the business interests by ensuring the recruitment of the right resources, educating the employees of cybersecurity risks, and complying with the code of conduct.

Human resource must be aware of the risk posture of an entity. It shall implement the appropriate security controls by defining contracts, administration procedures, and technology to minimize the exposure to the threats.

The motive of Human resource security should be, but not limited to:

- Defining Disciplinary processes
- Background verification
- Security Awareness and Training
- Privilege Management
- Defining Roles & Responsibilities
- Transition Management

The common threats posed to an entity, employees, or contractors having access to PII or PHI can be:

- Social Engineering
- Accidental Leakage
- Privilege Abuse
- Spear Phishing
- Intentional Leakage
- Human Errors

The objective is to ensure that all employees, contractors, or any user handling or exposed to PII, PHI, or any sensitive data are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated. The primary Human Resources security measures are taken during the phases:

- Before Employment
- During Employment
- Termination or Transitions in Roles

<table>
<tr><th colspan="4">Major Control: HRS 1.1: Human Resources Security Policy</th></tr>
<tr><td colspan="2">HRS1.1.1</td><td colspan="2">Basic</td></tr>
<tr><td colspan="2"><b>Human Resource Security Policy</b></td><td>Control Type</td><td>Management</td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity must develop, enforce and maintain a human resources security policy covering the security aspects of employment and termination</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The policy shall:
• Define management requirements on:
○ Background verification for employees and contractors
○ Roles and responsibilities
○ Compliance with acceptable usage and other organizational security policies
○ Training and awareness needs
○ Return of assets during exit
• Mandate the requirements of non-disclosure and confidentiality during and after employment
• Include reference to the organizational disciplinary process</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> M3.1.1, M4.1.1
<b>ISO27001:2013:</b> A.6.1.1
<b>NIST800-53 Rev4:</b> PS-1</td></tr>
</table>

Major Control: HRS 1.2: Prior to the Employment		
HRS1.2.1	Basic	
Background Verification Check	Control Type	Management

Sub-Control	The entity shall conduct background verification checks on all candidates for employment, contractors, and third-party users

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The entity shall:

- Define background verification process addressing provisions of government mandates and entity demands
- Establish criteria for background verification checks based on:
    - Role of the individual
    - Classification of information access needed
    - Access to critical areas
    - Risk identified

Control Reference	**UAE IA:** M4.2.1 **ISO27001:2013:** A.7.1.1 **NIST800-53 Rev4:** PS-3

HRS1.2.2	Basic	
Terms and Condition of Employment	Control Type	Management

Sub-Control	The entity shall establish specific terms and conditions of employment.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

<table>
<tr><td colspan="2">The terms and condition shall:
• Include control requirement specific to employees, contractors, and third parties, relevant to their roles and risk profiles
• Include information security responsibilities of the entity and the employees, contractors, and third parties
• Include standard information security requirements
• Be read, understood, agreed and signed by employees, contractors, and third parties
• The entity shall conduct mandatory briefing sessions to employees, contractors, and third parties on standard and specific information security requirements of the terms and condition
• Maintain adequate records on the employee, contractor, and third-party briefing
• Maintain terms and conditions signed by the employee, contractor, and third-party resources in-line with entity retention requirements</td></tr>
<tr><td><b>Control Reference</b></td><td><b>UAE IA:</b> M4.2.2
<b>ISO27001:2013:</b> A.7.1.2
<b>NIST800-53 Rev4:</b> AC-20, PL-4, PS-6, PS-7</td></tr>
</table>

<table>
<tr><td colspan="4"><b>Major Control: HRS 1.3: During Employment</b></td></tr>
<tr><td colspan="2"><b>HRS1.3.1</b></td><td colspan="2">Basic</td></tr>
<tr><td colspan="2"><b>Compliance to Organizational Policies and Procedures</b></td><td><b>Control Type</b></td><td>Management</td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity management shall ensure that employees, contractors, and third-party users adopt and apply security per established entity policies and procedures</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The entity shall:
• Ensure that employees, contractors, and third-party users are briefed on the entity’s information security compliance requirements
• Establish acceptable usage policy and ensure users read, accept and sign the policy before the provision of a system, application, or information access
• Consider segregation of duties to avoid potential misuse of position or conflict of interest</td></tr>
<tr><td colspan="2"><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> M4.3.1
<b>ISO27001:2013:</b> A.18.2.2
<b>NIST800-53 Rev4:</b> PL-4, PS-6, PS-7, SA-9</td></tr>
</table>

HRS1.3.2	Basic	
Cybersecurity Training	**Control Type**	Technical
Sub-Control	The entity shall identify and address skill and competency, demands and gaps	
• IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall: • Assess and identify skill and competency gaps on information security demands • Implement skill and competency development programs		
Control Reference	**UAE IA:** M3.2.1, M3.3.3, M3.3.4, M3.3.5 M3.3.1, M3.3.2 **ISO27001:2013:** A.7.2.2 **NIST800-53 Rev4:** AT-3 **CIS CSC 7.1** : 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8. 17.9	
HRS1.3.3	Basic	
Awareness Campaign	**Control Type**	**Management**
Sub-Control	The entity shall develop new or modify existing awareness programs to include requirements of governmental and organizational information security demands	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall: • Ensure all employees and where relevant contractors and third parties receive appropriate awareness and training to enhance the entity's security posture and to minimize probabilities of information security risks • Ensure that an awareness and training program is formally launched and professionally managed • Enhance training contents and enrich the delivery of awareness aspects based on evolving needs • Evaluate effectiveness and maintain an appropriate record of awareness and training delivered		
Control Reference	**UAE IA:** M3.4.1 **ISO27001:2013:** A.7.2.2 **NIST800-53 Rev4:** AT-3 **CIS CSC 7.1** : 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8. 17.9	

HRS1.3.4	Foundational	
Disciplinary Process	**Control Type**	**Management**
Sub-Control	The entity shall establish and enforce a disciplinary process for employees, where relevant contractors and third parties, who have committed security breaches	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall: • Ensure employees, contractors and third-party resources are aware of the entity's disciplinary processes • Enforce disciplinary processes and maintain necessary records on the breaches and management's actions		
Control Reference	**UAE IA:** M3.4.2 **ISO27001:2013:** A.7.2.3 **NIST800-53 Rev4:** PS-8	

Major Control: HRS 1.4 Termination or Change of Employment and Role		
HRS1.4.1	Basic	
Termination Responsibility	Control Type	Management
Sub-Control	The entity shall define responsibilities concerning information security for performing employment termination or change of employment	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity must: • Establish internal and external communication protocol on employment exit • Ensure adequate knowledge transfers and responsibility handovers		
Control Reference	**UAE IA:** M4.4.1 **ISO27001:2013:** A.7.3.1 **NIST800-53 Rev4:** PS-4, PS-5 **CIS CSC 7.1** : 16.8, 16.9	
HRS1.4.2	Basic	
Return of Assets	Control Type	**Management**
Sub-Control	The entity shall ensure recovery of all organizational assets upon termination of employment, contract, or agreement	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity must: • Ensure all organizational assets are recovered and necessary acknowledgement and clearance obtained from appropriate stakeholders • Ensure all information, with particular focus on PHI information, has been recovered and cannot be misused anywhere, anytime • Ensure resources leaving the entity formally acknowledges and confirms that no information is under their direct or indirect possession or use		
Control Reference	**UAE IA:** M4.4.2 **ISO27001:2013:** A.8.1.4 **NIST800-53 Rev4:** PS-4, PS-5 **CIS CSC 7.1** : 1.6	

HRS1.4.3		Basic	
Removal of Access Rights		**Control Type**	**Technical**
Sub-Control	The entity shall remove access to systems, applications, information, secure areas, and work areas.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
The entity to: • Ensure access to systems, application, information, secure areas, work areas, and identified critical areas are revoked upon termination • Communicate with MOHAP to revoke any relevant system and application access upon termination			
Control Reference		**UAE IA:** M4.4.3 **ISO27001:2013:** A.9.2.1 **NIST800-53 Rev4:** AC-2, PS-4, PS-5 **CIS CSC 7.1** : 16.6	
HRS1.4.4		Basic	
Internal Transfers and Change Of Role		**Control Type**	**Technical**
Sub-Control	The entity shall remove access to systems, applications, information, secure areas, and work areas.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
The entity to: • Ensure communication to all necessary internal and external stakeholders on change of role or internal transfers • Revoke access and privileges associated with the old role and reassign privileges on the system, application, and information access and utilization consistent with their new role based on necessary authorization			
Control Reference		**UAE IA:** M4.4.3 **ISO27001:2013:** A.9.2.1 **NIST800-53 Rev4:** AC-2, PS-4, PS-5 **CIS CSC 7.1** : 16.6	

5.2. Asset Management

In the age of ever-changing business environment, the Healthcare sector has observed a revolution of connected information systems assets bringing IOT assets onboard. To maintain the availability of such assets to support critical business functions and the information available, it is the entity’s responsibility to implement appropriate security controls to mitigate risks posed to the information assets.

The business units and management must be aware of the available assets in the entity in any form available to implement security around them. The following are the type of assets a business may possess.

- Information/Data (Tangible)
- Applications or Software
- Physical Assets (HVAC, DC, Electric)
- Human Resource
- Information/Data (non-Tangible)
- Information Systems
- Medical Equipment
- Industrial Control Systems

The common threats posed to an entity which can compromise the asset with PII or PHI can be:

- Denial of Service
- Unauthorized Access/Abuse
- Information Theft
- Embezzlement/Fraud
- System Malfunction
- Retrieval of Discarded Media

The objective is to ensure to develop and maintain a risk-based structure establishing the strategies and parameters of the activities and procedures to identify and protect information assets from potential threats focusing on the business and healthcare information and ensure the confidentiality, integrity, and availability of information systems. The significant objectives may include:

- Compliance Policies
- Asset Classification & Management
- Asset Handling & Destruction

Major Control: ASM2.1 Asset Management Policy

<table>
<tr><td colspan="2"><b>ASM 2.1.1</b></td><td colspan="2">Basic</td></tr>
<tr><td colspan="2"><b>Asset Management Policy</b></td><td><b>Control Type</b></td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">An entity shall develop, implement, and maintain an asset management policy for medical equipment and devices while defining policy, and shall categorically address the following:</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The management policy must:
• Be relevant and appropriate for entities operational and risk environment
• Establish a framework to effectively manage the entity’s information assets through ownership assignment, accountability & responsibility definition, recording and maintaining of all/relevant properties of asset
• Define roles and responsibilities for actions expected out of asset management policy, and shall have functional KPI’s for business/function leaders
• Define and enforce classification schemes, as applicable for MOHAP (Public, Restricted, Confidential & Secret)
• Identify the requirements of data retention, handling, and disposal
• Have provisions for managing Bring Your Own Device (BYOD) arrangements
• Be reviewed, updated, and maintained at planned intervals or during significant changes to operating or risk environment, whichever is earlier
• Be approved by the entity’s top management or its head and shall be communicated to all employees and third parties having a role in care delivery
• Roles that will be allowed to access, use and maintain medical devices and equipment shall be established
• To the extent possible, medical devices and equipment to authenticate users, based on entity authentication and authorization process
• The need for handling procedures for each medical device and equipment in use shall be defined and updated as required to stay current
• The need to establish and maintain risk log concerning medical devices and equipment
• Decommissioning and/or disposal of medical devices and equipment</td></tr>
<tr><td colspan="2"><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> T.1.1.1
<b>ISO27001:2013:</b> A.8.1.1
<b>NIST800-53 Rev4:</b> MP-1, CM-1
<b>CIS CSC 7.1 :</b> 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.4, 15.1, 16.1</td></tr>
</table>

Major Control: ASM 2.2 Management of Asset		
ASM 2.2.1	Basic	
Asset Inventory	Control Type	Technical
Sub-Control	The entity shall have all its information assets identified and maintained through an information asset inventory system.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The inventory must include: • The inventory shall be updated periodically, or during the change in the environment, and shall be accurate and reliable • The inventory can be centralized or distributed (function/line-of-business/service wise) based on the entity's internal structures and shall be updated • The inventory shall establish the relations between various types of information assets, in support of care delivery		
Control Reference	**UAE IA:** T.1.2.1 **ISO27001:2013:** A.8.1.1 **NIST800-53 Rev4:** CM-8, CM-9, PM-5 **CIS CSC 7.1 :** 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.4, 15.1, 16.1	
ASM 2.2.2	Basic	
Asset Ownership	Control Type	Management
Sub-Control	Ownership for each identified asset shall be assigned to a designated role	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
An entity must: • The owner of an information asset shall define/identify the control requirements to minimize the impact of risk, due to the compromise of assets under his ownership • The owner shall review the adequacy of implemented control measures periodically and amend/modify the control environment as necessary • The owner shall ensure the effectiveness of the implemented controls, in addressing the risk environment • The asset owner shall authorize access and/or use of information assets		

<table>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T.1.2.2
<b>ISO27001:2013:</b> A.8.1.2
<b>NIST800-53 Rev4:</b> CM-8, CM-9, PM-5
<b>CIS CSC 7.1 :</b> 1.5</td></tr>
<tr><td colspan="2">ASM 2.2.3</td><td colspan="2">Basic</td></tr>
<tr><td colspan="2"><b>Usage Acceptability of Assets</b></td><td>Control Type</td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">An entity shall establish and enforce rules on the acceptable use of information assets</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The policy must include:
• The rules shall be communicated to all employees and contractors in support of care delivery, and shall be read and acknowledged by all
• Entities shall maintain records of user acceptance on the acceptable use of information assets</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T.1.2.3
<b>ISO27001:2013:</b> A.8.1.3
<b>NIST800-53 Rev4:</b> AC-20, PL-4
<b>CIS CSC 7.1 :</b> 5.1, 7.1, 15.4, 15.5, 15.6, 15.9, 16.11</td></tr>
<tr><td colspan="2">ASM 2.2.4</td><td colspan="2">Basic</td></tr>
<tr><td colspan="2"><b>Acceptable Bring Your Own Device Arrangements</b></td><td>Control Type</td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">Entity management shall be aware of risks and must address risk due to the exploitation of the Bring Your Own Device (BYOD).</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The policy must include:
• Probabilities of compromise by personal devices shall be addressed through suitable rules and role-based usage agreements
• Authorization to use personal devices to access/view/use/share/process/store personal health information (PHI) is subject to user acknowledgement on the usage agreements.</td></tr>
</table>

Control Reference	**UAE IA:** T.1.2.4 **ISO27001:2013:** A.6.2.1 **NIST800-53 Rev4:** IA-8, AC-20 **CIS CSC 7.1 :** 13.6

Major Control: ASM 2.3 Asset Classification & Labelling		
ASM 2.3.1	Basic	
Information Classification and Re-Classification	Control Type	**Management**
Sub-Control	The entity shall classify all information assets, that categorizes information assets:	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The information assets must be classified according to the industry requirements. Organizations should have 3-4 classification options to allow effective management of the information considering its value and importance. It can, however, be as simple or as complex as required to ensure the correct level of granularity for the protection of assets. A process must be established to classification and re-classification of the information assets based on assessment or change in the category of an information asset based on the following. • Change in the value of information • Changes to the environment (Access, applications, permissions, etc.) • Changes in protection levels (**Optional**) To achieve a higher level of maturity, the automated tools/technology to classify the information should be considered based on established information classification policy, schema, and criteria.		
Control Reference	**UAE IA:** T.1.3.1 **ISO27001:2013:** A.8.2.1 **NIST800-53 Rev4:** RA-2 **CIS CSC 7.1:** 13.1	
ASM 2.3.2	Foundational	
Information Valuation, Protection, and Classification Schema	Control Type	**Technical**
Sub-Control	The entity must classify the information assets based on value, implement protection	

	controls, and categorize as per business risk posture.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Information classification must consider the value of the information and be more restrictive based on the entity's risk posture considering the compromise of the information classified. The classification must be assigned the essential protection controls based on the valuation. The classification schema can be consisted of the categories below or based on industry-standard being followed, example categories such as: • Public • Internal • Confidential • Restricted		
Control Reference	**UAE IA:** T.1.3.1 **ISO27001:2013:** A.8.2.1 **NIST800-53 Rev4:** RA-2 **CIS CSC 7.1:** 13.1	
ASM 2.3.3	**Basic**	
Asset Labeling	**Control Type**	**Technical**
Sub-Control	The entity must establish a process of labelling of business assets.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Asset labelling process should be defined based on the identification, valuation, and classification for the asset types, such as: • Physical • Digital		
Control Reference	**UAE IA:** T.1.3.2 **ISO27001:2013:** A.8.2.2 **NIST800-53 Rev4:** AC-16, MP-2, MP-3, SC-16 **CIS CSC 7.1 :** 1.4	

Major Control: ASM 2.4 Asset Handling			
ASM 2.4.1		Basic	
Asset Handling Procedures		Control Type	**Technical**
Sub-Control	The entity shall define asset handling procedures based on the classification:		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
The asset handling procedures must be defined and enforced according to the classification assigned to information assets. Handling procedures shall consider the processing phases of information such as: • Privilege Allocation. • Transit • Storage • Processing			
Control Reference		**UAE IA:** T.1.3.3 **ISO27001:2013:** A.7.2.2 **NIST800-53 Rev4:** AC-16, MP-2, MP-3, SC-16 **CIS CSC 7.1 :** 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8. 17.9	
ASM 2.4.2		Basic	
Management of Removable Media		Control Type	**Technical**
Sub-Control	The entity must manage and enforce policies for removable media per classification.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
Policies to manage the removable media should be defined as per the asset classification and handling procedures to determine the acceptable usage policy. The policy should consist of: • Media management procedures. • Media lifecycle management • Protection against unauthorized access. • Protection against embezzlement or alteration Management must authorize the usage of the removable media, inherit/accept the risks associated with usage of removable media, and be held accountable for the usage of removable media.			

<table>
<tr><td colspan="4">(<b>Optional</b>) To achieve a higher level of maturity in removable media management, the entity should consider implement device tagging, whitelisting to enable encryption, and authorized device provisioning.</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T.1.4.1
<b>ISO27001:2013:</b> A.10.7.1
<b>NIST800-53 Rev4:</b> MP Family, PE-16
<b>CIS CSC 7.1 :</b> 13.7, 13.8</td></tr>
<tr><td colspan="2"><b>ASM 2.4.3</b></td><td colspan="2"><b>Foundational</b></td></tr>
<tr><td colspan="2"><b>Removal and Movement of Information Assets</b></td><td><b>Control Type</b></td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity must establish appropriate procedures of removal, transition, and movement of information assets.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">Procedures must be established to manage the removal, transportation, transition, and movement of the information asset types such as:
• Data/Information
• Equipment (Medical/Non-Medical)
• Information system

The process must include the following:
• Authorization of removal
• Movements and transfer
• Tracking and Record Maintenance</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T.2.3.7
<b>ISO27001:2013:</b> A.9.2.7
<b>NIST800-53 Rev4:</b> MP-5, PE-16</td></tr>
</table>

Major Control: ASM 2.5 Asset Disposal		
ASM 2.5.1	**Basic**	
Secure Information Asset or Media Disposal	**Control Type**	**Technical**
Sub-Control	The entity to establish the procedure for securely disposing of the information assets.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity must establish the procedures to securely dispose-off information assets in the events of: • Not Needed by Entity • Regulatory Requirements • Legal Requirements The facility must verify the following before disposal of physical or digital assets: • Sensitive Data, licensed software is removed or destroyed and not recoverable • Data Retention requirement has been fulfilled to retain backups or archives The facility ensures that the management must authorize and approve the disposal of the assets.		
Control Reference	**UAE IA:** T.1.4.2 **ISO27001:2013:** A.10.7.2 **NIST800-53 Rev4:** MP-6	
ASM 2.5.2	**Foundational**	
Procedures for Re-Use of Assets	**Control Type**	**Management**
Sub-Control	The facility must establish and implement the procedures to re-use the information assets.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The facility must establish control procedures reuse of media, equipment, devices, and systems, containing classified information, implement procedures such as: • Storage media shall be verified to ensure it is free of sensitive information • Keep traceability of sensitive disposed items by keeping logs. • Use the disposal checklist to ensure that critical elements are verified.		

<table>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T.2.3.6
<b>ISO27001:2013:</b> A.9.2.6
<b>NIST800-53 Rev4:</b> MP-6
<b>CIS CSC 7.1:</b> 16.7</td></tr>
<tr><td colspan="2"><b>ASM 2.5.3</b></td><td colspan="2"><b>Organizational</b></td></tr>
<tr><td colspan="2"><b>Records on Disposal</b></td><td><b>Control Type</b></td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity shall maintain records, on media disposal.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The entity must maintain records, on media disposal. The records ideally have, the following fields:
• Owner Information
• Media Type
• Asset Classification
• Disposal Procedure
• Reason for disposal
• Retention Limit of data
• Data removal evidence
• Disposal authorized evidence</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T.2.3.7
<b>ISO27001:2013:</b> A.9.2.7
<b>NIST800-53 Rev4:</b> MP-5, PE-16</td></tr>
</table>

5.3. Physical and Environmental Security

Physical and environmental safeguards are often overlooked but are very important in protecting information and critical infrastructure in the healthcare sector. Physical security has become increasingly difficult in the modern, complex, and dynamic organizations due to workforce mobility, portability, and mobile access. Information systems and medical equipment must be afforded appropriate protection to avoid damage or unauthorized access.

The environmental factors must be considered to protect the vested interest of healthcare organizations to prevent or minimize the impact of fire, flood, intentional destruction, unintentional damage, mechanical failure, power failure.

Physical security measures shall be implemented to deal with the risks an organization may be exposed to and periodically tested, such as:

- Physical Security Compliance Policy
- Physical Security Awareness
- Information Systems Infrastructure Security
- Perimeters Security
- Medical Equipment Security
- Planning and Protection against Environmental Threats

The common threats a healthcare facility might be exposed to can be:

- Theft or Vandalism
- Tempering or Destruction
- Power or Mechanical Failure
- Unauthorized Access
- Environmental Threats
- Physical Intrusion

The objective is to ensure the healthcare facility shall be protected against physical and environmental threats and prevent damages to the facility’s critical assets from any breaches or accidents. The protection controls include:

- Security Policy
- Facility Security
- Equipment Security

Major Control: PHE 3.1 Physical and Environmental Security Policy		
PHE 3.1.1	Basic	
Management Policy for Physical and Environmental Security	Control Type	**Management**
Sub-Control	A management security policy must be developed by the entity addressing the Physical and Environmental aspects of information security.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The management policy must facilitate the implementation of the associated controls and reduce probabilities of risk realization of Physical and Environmental threats covering aspects such as:

- Identify risk elements of the physical security of the entity for internal or external threats.
- Secure storage requirements for anything hazardous to an entity's operations or environment, potentially harmful to humans risking for any injury or fatality, has the potential to damage information systems or processing facilities.
- Prioritization of assets according to the value to the assets and propose appropriate controls.

The policy must be

- Read by all users and acknowledged.
- Reviewed and updated for any major updates according to risk landscape.

The Management policy for physical and environmental security must be reviewed by top management of disaster management, information systems management, or any relevant departments before communicated with all the employees and third parties.

The entity should also establish the process to enforce the policy while considering the below:

- Equipment Physical access.
- Recommended Controlled environment for specific equipment by the MOHAP or Vendors.
- Prevention of the Loss/Leakage of information or data due to unauthorized access

Control Reference	**UAE IA:** T2.1.1, T2.3.5 **ISO27001:2013:** A.11.1.1 **NIST800-53 Rev4:** AC-19, AC-20, MP-5, PE-17

<table>
<tr><th colspan="4">Major Control: PHE 3.2 Secure or Restricted Areas</th></tr>
<tr><td colspan="2">PHE 3.2.1</td><td colspan="2">Basic</td></tr>
<tr><td colspan="2">Physical Security Perimeter</td><td>Control Type</td><td>Technical</td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity must define the Security perimeters and use it to protect areas that contain either sensitive or critical information and information processing facilities.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The entity shall follow the guidelines below and consider implementing where appropriate for physical security perimeters, such as:
• Security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment.
• Perimeters of a building or site containing information processing facilities should be physically sound [i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur]. The exterior roof, walls, and flooring of the site should be of solid construction, and all external doors should be suitably protected against unauthorized access with control mechanisms, ‘ (e.g. bars, alarms, locks). Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.
• A manned reception area or other means to control physical access to the site or building should be in place. Access to sites and buildings should be restricted to authorized personnel only.
• Physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination.
• All fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national, and international standards. They should operate in accordance with the local fire code in a failsafe manner.
• Suitable intruder detection systems should be installed to national, regional, or international standards and regularly tested to cover all external doors and accessible windows. Unoccupied areas should always be alarmed. The cover should also be provided for other areas,’e.g. Data centres, Healthcare labs, etc. ‘
• Information processing facilities managed by the organization should be physically separated from those managed by external parties.</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T2.2.1
<b>ISO27001:2013:</b> A.11.1.1
<b>NIST800-53 Rev4:</b> PE-1</td></tr>
<tr><td colspan="2">PHE 3.2.2</td><td colspan="2">Foundational</td></tr>
<tr><td colspan="2">Secure Areas Control Measures</td><td>Control Type</td><td>Technical</td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity must secure areas with appropriately protected on entry to ensure that only authorized personnel are allowed access.</td></tr>
</table>

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The following guidelines should be considered:

- The timestamp of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved. They should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and emergency procedures. The identity of visitors should be authenticated by an appropriate means.
- Access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN.
- A physical logbook or electronic audit trail of all access should be securely maintained and monitored.
- All employees, contractors, and external parties should be required to wear some form of visible identification. They should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.
- External party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required: this access should be authorized and monitored.
- Access rights to secure areas should be regularly reviewed and updated and revoked when necessary

Control Reference	**UAE IA:** T2.2.3 **ISO27001:2013:** A.11.1.3 **NIST800-53 Rev4:** PE-3, PE-4, PE-5
PHE 3.2.3	Basic

Secure Office & Meeting Rooms	Control Type	**Technical**

Sub-Control	Physical security for offices, rooms, and facilities should be designed and applied.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The following guidelines should be considered to secure offices, rooms, and facilities:

- Key facilities should be sited to avoid access by the public.
- Where applicable, buildings should be unobtrusive and give a minimum indication of their purpose, with no apparent signs, outside or inside the building, identifying the presence of information processing activities.
- Facilities should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate.
- Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

Control Reference	**UAE IA:** T2.2.3 **ISO27001:2013:** A.11.1.3 **NIST800-53 Rev4:** PE-3, PE-4, PE-5

PHE 3.2.4	Basic	
Protection against External & Environmental Threats	Control Type	**Technical**
Sub-Control	The entity should consider implementing controls for physical protection against natural disasters, malicious attack or accidents should be designed and applied.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Specialist advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. The following actions can be taken: • Availability of the parallel processing equipment or facility consistent with devices, systems, and backup media are protected from damage caused by natural or man-made disasters or accidents. • Backup power such as Uninterrupted power supply, Electricity generators must be available to power up the key information systems and critical data centre infrastructures.		
Control Reference	**UAE IA:** T2.2.4 **ISO27001:2013:** A.11.1.4 **NIST800-53 Rev4:** CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15	
PHE 3.2.5	**Foundational**	
Effectiveness of Control Measures	Control Type	**Management**
Sub-Control	The entity must ensure the physical security measures taken are implemented and audited.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity must ensure that the physical security measure and controls are implemented effectively with the measures below: • Table-top exercises to ensure the policies are in place. • Independent audits by external firms to assess the security measures in place to identify the vulnerabilities. • Drill exercises to test run the back-up facilities, systems, power supplies for critical infrastructure.		
Control Reference	**UAE IA:** T2.2.4 **ISO27001:2013:** A.11.1.4 **NIST800-53 Rev4:** CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15	
PHE 3.2.6	Basic	

Working in Secure Areas	**Control Type**	**Management**
Sub-Control	The entity must define and implement procedures for working in secure areas.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The following guidelines should be considered: • Personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis. • Unsupervised working in secure areas should be avoided both for safety reasons and to prevent • Opportunities for malicious activities. • Vacant secure areas should be physically locked and periodically reviewed. • Photographic, video, audio, or other recording equipment, such as cameras in mobile devices, should not be allowed unless authorized.		
Control Reference	**UAE IA:** T2.2.5 **ISO27001:2013:** A.11.1.5 **NIST800-53 Rev4:** AT-2, AT-3, PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8	
PHE 3.2.7	**Foundational**	
Physical Security Awareness	**Control Type**	**Management**
Sub-Control	The entity should establish an awareness program for physical security and a secure workplace environment.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Physical security awareness can include the following: • Workshops by management to raise awareness of a secure working environment and physical security. • Activities to raise awareness among employees, stakeholders, and partners to ensure up to date knowledge of people.		
Control Reference	**UAE IA:** T2.2.5 **ISO27001:2013:** A.11.1.5 **NIST800-53 Rev4:** AT-2, AT-3, PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8 **CIS CSC 7.1:** 17.3	
PHE 3.2.8	**Basic**	
Delivery and Loading Areas	**Control Type**	**Management**
Sub-Control	The entity should ensure the access control is implemented in areas such as loading bays,	

	delivery access points, etc.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access, the guidelines below should be considered:

- Access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel.
- The delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building.
- The external doors of a delivery and loading area should be secured when the internal doors are opened.
- The incoming material should be inspected and examined for explosives, chemicals, or other hazardous materials before it is moved from a delivery and loading area.
- The incoming material should be registered in accordance with asset management procedures on entry to the site.
- Incoming and outgoing shipments should be physically segregated, where possible.
- The incoming material should be inspected for evidence of tampering en route. If such tampering is discovered, it should be immediately reported to security personnel.

Control Reference	**UAE IA:** T2.2.6 **ISO27001:2013:** A.11.1.6 **NIST800-53 Rev4:** PE-3, PE-7, PE-16

Major Control: PHE 3.3 Equipment Security		
PHE 3.3.1	Basic	
Equipment siting and protection	Control Type	**Technical**
Sub-Control	The entity should make the appropriate arrangements that equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The following guidelines should be considered to protect equipment:

- Equipment should be sited to minimize unnecessary access to work areas.
- Information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use.
- Storage facilities should be secured to avoid unauthorized access.

- Items requiring special protection should be safeguarded to reduce the general level of protection required.
- Controls should be adopted to minimize the risk of potential physical and environmental threats. e.g. theft, fire explosives, smoke, water (or water supply failure), dust, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.
- Guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established.
- Environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.
- Lightning protection should be applied to all buildings, and lightning protection filters should be fitted to all incoming power and communications lines.
- The use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments.
- Equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

Control Reference	**UAE IA:** T2.3.1 **ISO27001:2013:** A.11.2.1 **NIST800-53 Rev4:** PE-1, PE-18 **CIS CSC 7.1** : 1.6
PHE 3.3.2	**Foundational**

Supporting Utilities	**Control Type**	**Technical**

Sub-Control	The Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation, and air conditioning) should:

- Conform to equipment manufacturer's specifications and local legal requirements:
- Be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities.
- Be inspected and tested regularly to ensure their proper functioning.
- If necessary, be alarmed to detect malfunctions.
- If necessary, have multiple feeds with diverse physical routing.

Control Reference	**UAE IA:** T2.3.2 **ISO27001:2013:** A.11.2.2 **NIST800-53 Rev4:** PE-1, PE-9, PE-11, PE-12, PE-14

PHE 3.3.3		Basic	
Cabling Security		Control Type	Technical
Sub-Control	Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference, or damage.		

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

- The entity should consider the following guidelines for cabling security:
  - Power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection.
  - Power cables should be segregated from communications cables to prevent interference:
  - For sensitive or critical systems further controls to consider include:
    - Installation of armoured conduit and locked rooms or boxes at inspection and termination points.
    - Use of electromagnetic shielding to protect the cables.
    - Initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables.
    - Controlled access to patch panels and cable rooms

Control Reference	**UAE IA:** T2.3.3 **ISO27001:2013:** A.11.2.3 **NIST800-53 Rev4:** PE-4, PE-9

PHE 3.3.4		Organizational	
Equipment Maintenance		Control Type	Technical
Sub-Control	Equipment should be correctly maintained to ensure its continued availability and integrity.		

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The following guidelines for equipment maintenance should be considered:

- Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.
- Only authorized maintenance personnel should carry out repairs and service equipment.
- Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.
- Appropriate controls should be implemented when equipment is scheduled for maintenance, considering whether this maintenance is performed by personnel on-site or external to the
- Organization where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared.

- All maintenance requirements imposed by insurance policies should be complied with.
- Before putting equipment back into operation after its maintenance, it should be inspected to ensure that the equipment has not been tampered with and does not a malfunction.

Control Reference	**UAE IA:** T2.3.4 **ISO27001:2013:** A.11.2.4 **NIST800-53 Rev4:** MA Family **CIS CSC 7.1** : 1.6	
PHE 3.3.5	**Foundational**	
Removal of Equipment	Control Type	**Technical**
Sub-Control	Equipment or any physical assets should not be taken off-site without prior authorization.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The following guidelines should be considered

- Employees and external party users who have the authority to permit off-site removal of assets should be identified.
- Time limits for asset removal should be set, and returns are verified for compliance.
- Where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned.
- The identity, role, and affiliation of anyone who handles or uses assets should be documented, and this documentation returned with the equipment or any physical assets.

Control Reference	**UAE IA:** T2.3.5 **ISO27001:2013:** A.11.2.5 **NIST800-53 Rev4:** MP-5 **CIS CSC 7.1** : 1.6	
PHE 3.3.6	**Organizational**	
Security of Equipment Off-premises	Control Type	**Technical**
Sub-Control	Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The use of any information storing and processing equipment outside the organization's premises should be authorized by management. This applies to equipment owned by the organization and that equipment owned privately and used on behalf of the organization. The following guidelines should be considered for the protection of off-site equipment:

- Equipment and media taken off-premises should not be left unattended in public places.
- Manufacturers' instructions for protecting equipment should always be observed, e.g. protection against exposure to strong electromagnetic fields.
- Controls for off-premises locations, such as home-working, teleworking, and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers, and secure communication with the office
- Chen off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.

Control Reference	**UAE IA:** T2.3.7 **ISO27001:2013:** A.11.2.6 **NIST800-53 Rev4:** PE-17, PE-16 **CIS CSC 7.1** : 1.6
PHE 3.3.7	**Foundational**

Secure disposal or re-use of equipment	Control Type	**Technical**

Sub-Control	All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Damaged equipment containing storage media may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment. Besides, to secure disk erasure, whole-disk encryption reduces the risk of disclosure of- confidential information when equipment is disposed of or redeployed, provided that:

- The encryption process is sufficiently strong and covers the entire disk, including slack space, swap files, etc.
- The encryption keys are long 'enough to resist brute force attacks.
- The encryption keys are themselves kept confidential (e.g. never stored on the same disk).

Control Reference	**UAE IA:** T.2.3.6 **ISO27001:2013:** A.11.2.7 **NIST800-53 Rev4:** MP-6, SA-19(3)
PHE 3.3.8	**Basic**

Unattended User Equipment	Control Type	**Technical**
Sub-Control	Equipment or any physical assets should not be taken off-site without prior authorization.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Users should ensure that unattended equipment has appropriate protection. All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

- Terminate active sessions when finished unless they can be secured by an appropriate locking mechanism such as a password-protected screen saver.
- Log-off from applications or network services when no longer needed.
- Secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

Control Reference	**UAE IA:** T.2.3.8 **ISO27001:2013:** A.11.2.8 **NIST800-53 Rev4:** AC-11, IA-2, PE-3, PE-5, PE-18, SC-10
PHE 3.3.9	Basic

Clear Desk & Clear Screen Policy	Control Type	**Technical**
Sub-Control	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The clear desk and clear screen policy should consider the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:

- Sensitive or critical business information, e.g. on paper or electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required especially when the office is vacated.
- Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords, or other controls when not in use.
- Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented.
- Media containing sensitive or classified information should be removed from printers immediately.

Control Reference	**UAE IA:** T.2.3.9 **ISO27001:2013:** A.11.2.9 **NIST800-53 Rev4:** AC-11

5.4. Access Control Management

The access control management is considered an integral part of any cybersecurity program, hence considered crucial for any healthcare facility to ensure safeguards implementation for access management to the information processing systems responsibly to affirm their commitment to MOHAP strategic cybersecurity goals.

With the key reliance of healthcare facilities on information technology to deliver the services and perform crucial business functions, it is essential to recognize the responsibility of access management to ensure the confidentiality, integrity, and availability of Personal Identifiable and Healthcare information and prevent unauthorized access to affirm the public trust in their services. Implement accountability measures to detect and prevent breaches and hold accountable for any consequences.

The healthcare facility shall mandate the policies, procedures, and appropriate controls to ensure the protection of information being processed by itself or behalf of MOHAP, which may include:

- Access Control Compliance Policies
- Access to Medical Equipment and Information
- Network and Systems Access Management
- Secure Credential Management
- Access & Privilege Management
- Accountability and Access Reviews
- Applications Access Management
- Authentication and Authorization Management
- Archival Access Protection

The common threats based on risk management, a healthcare information processing facility may be vulnerable to can be:

- Unauthorized Access
- Misappropriation of knowledge
- Lack of accountability processes
- Abuse of Privileges
- Tampering of Media
- Identity Breaches

The objective is to ensure limited access to information and information processing facilities, authorized user access and to prevent unauthorized access to systems and services, make users accountable for safeguarding their authentication information, and prevent unauthorized access to systems and applications. The controls may include:

- Compliance Policies
- Identity and Access Management
- Accountability of Access

Major Control: ACM 4.1 Access Control Policy		
ACM 4.1.1	**Basic**	
Access Control Policy	**Control Type**	**Management**
Sub-Control	The entity must define, establish, document, and review an access control policy based on business and information security requirements.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Asset owners should determine appropriate access control rules, access rights, and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks. Access controls are both logical and physical, and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls. The policy should take account of the following:

- Security requirements of business applications.
- Policies for information dissemination and authorization, e.g. the need-to-know principle and information security levels and classification of information.
- Consistency between the access rights and information classification policies of systems and networks.
- Relevant legislation and any contractual obligations regarding the limitation of access to data or services.
- Management of access rights in a distributed and networked environment that recognizes all types of connections available.
- Segregation of access control roles, e.g. access request, access authorization, access administration.
- Requirements for formal authorization of access requests.
- Requirements for periodic review of access rights.
- Removal of access rights.
- Archiving of records of all significant events concerning the use and management of user identities and secret authentication information
- Roles with privileged access

Control Reference	**UAE IA:** T5.1.1 **ISO27001:2013:** A.9.1.1 **NIST800-53 Rev4:** AC-1 **CIS CSC 7.1** : 14.6

<table>
<tr><th colspan="4">Major Control: ACM 4.2 User Access Management</th></tr>
<tr><td colspan="2">ACM 4.2.1</td><td colspan="2">Basic</td></tr>
<tr><td colspan="2"><b>User Registration and De-Registration</b></td><td>Control Type</td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">Formal user registration and de-registration process should be implemented by the entity to enable the assignment of access rights.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The process for managing user IDs should include:
Using unique user IDs to enable users to be linked to and held responsible for their actions. The use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented.
• Immediately disabling or removing user IDs of users who have left the organization.
• Periodically identifying and removing or disabling redundant user IDs.
• Ensuring that redundant user IDs are not issued to other users.
Providing or revoking access to information or information processing facilities is usually a two-step procedure:
• Assigning and enabling, or revoking, a user ID.
• Providing, or revoking, access rights to such user ID.</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T5.2.1
<b>ISO27001:2013:</b> A.9.2.1
<b>NIST800-53 Rev4:</b> AC-1, AC-2, AC-21, IA-5, PE-1, PE-2
<b>CIS CSC 7.1</b> : 16.6</td></tr>
<tr><td colspan="2">ACM 4.2.2</td><td colspan="2">Organizational</td></tr>
<tr><td colspan="2"><b>Privilege Management</b></td><td>Control Type</td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The allocation and use of privileged access rights should be restricted and controlled by either my administration procedure or tools.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
</table>

The allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access control policy. The following steps should be considered:

- The privileged access rights associated with each system or process, e.g. operating system, database management system, and each application and the users to whom they need to be allocated should be identified.
- Privileged access rights should be allocated to users on a need-to-use basis and an event-by-event basis in line with the access control policy, i.e. based on the minimum requirement for their functional roles.
- An authorization process and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorization process is complete.
- Requirements for the expiry of privileged access rights should be defined.
- Privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged IDs.
- The competences of users with privileged access rights should be reviewed regularly to verify if they are in line with their duties.
- Specific procedures should be established and maintained to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities.
- For generic administration user IDs, the confidentiality of secret authentication information should be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

Control Reference	**UAE IA:** T5.2.2 **ISO27001:2013:** A.9.2.3 **NIST800-53 Rev4:** AC-1, AC-2, AC-6, AC-21, PE-1, PE-2, SI-9 **CIS CSC 7.1**: 4.3	
ACM 4.2.3	**Basic**	
Use and Management of Security Credential	**Control Type**	**Technical**
Sub-Control	The allocation of secret authentication information should be controlled through a formal management process.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The process should include the following requirements:

- Users should be required to sign a statement to keep personal secret authentication information confidential and to keep group (i.e. shared) secret authentication information solely within the members of the group; this signed statement may be included in the terms and conditions of employment.
- When users are required to maintain their secret authentication information, they should be provided initially with secure temporary secret authentication information`, which they are forced to change on first use.
- Procedures should be established to verify the identity of a user before providing a new, replacement, or temporary secret authentication information.
- Temporary secret authentication information should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided.

- Temporary secret authentication information should be unique to an individual and should not be guessable.
- Users should acknowledge receipt of secret authentication information.
- Default vendor secret authentication information should be altered following the installation of systems or software.

Control Reference	**UAE IA:** T5.2.3 **ISO27001:2013:** A.9.2.4 **NIST800-53 Rev4:** IA-5, IA-2 **CIS CSC 7.1** : 16.2, 16.4	
ACM 4.2.4	**Basic**	
Use of secret authentication information	**Control Type**	**Technical**
Sub-Control	Users should be required to follow the organization's practices in the use of secret authentication information.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

All users should be advised to:

- Keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority.
- Avoid keeping a record (e.g. on paper, software file, or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. password vault).
- Change secret authentication information whenever there is any indication of its possible compromise.
- When passwords are used as secret authentication information, select quality passwords with sufficient minimum length, which are:
    - Easy to remember
    - Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth, etc.
    - Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries).
    - Free of consecutive identical, all-numeric, or all-alphabetic characters.
    - If temporary, change at the first log-on.
- Not share individual user's secret authentication information.
- Ensure proper protection of passwords when passwords are used as secret authentication information in automated log-on procedures and are stored.
- Not use the same secret authentication information for business and non-business purposes.

Control Reference	**UAE IA:** T5.3.1 **ISO27001:2013:** A.9.3.1 **NIST800-53 Rev4:** IA-5 **CIS CSC 7.1**: 1.8	
ACM 4.2.5	**Basic**	
Password management system	**Control Type**	**Technical**
Sub-Control	Password management systems should be interactive and should ensure quality passwords.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

A password management system should:

- Enforce the use of individual user IDs and passwords to maintain accountability.
- Allow users to select and change their passwords and include a confirmation procedure to allow for input errors.
- Enforce a choice of quality passwords.
- Force users to change their passwords at the first log-on.
- Enforce regular password changes and as needed.
- Maintain a record of previously used passwords and prevent re-use.
- Not display passwords on the screen when being entered.
- Store password files separately from application system data.
- Store and transmit passwords in protected form.

Control Reference	**UAE IA:** T5.5.3 **ISO27001:2013:** A.9.4.3 **NIST800-53 Rev4:** IA-5 **CIS CSC 7.1** : 4.2, 4.4

Major Control: ACM 4.3 Equipment and Devices Access Control		
ACM 4.3.1	**Foundational**	
Access Control for Assets and Equipment in Teleworking Sites	**Control Type**	**Technical**
Sub-Control	A policy and supporting security measures should be implemented to protect information accessed processed or stored at teleworking sites.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

- The existing physical security of the teleworking site, considering the physical security of the building and the local environment.
- The proposed physical teleworking environment.
- The communications security requirements considering the need for remote access to the organization's internal systems. the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system.
- The provision of virtual desktop access that prevents the processing and storage of information on privately-owned equipment.
- The threat of unauthorized access to information or resources from other persons using the accommodation. e.g. family and friends.
- The use of home networks and requirements or restrictions on the configuration of wireless network services.
- Policies and procedures to prevent disputes concerning rights to intellectual property developed on privately-owned equipment.
- Access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation.
- Software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users.
- Malware protection and firewall requirements.

Control Reference	**UAE IA:** T5.7.2 **ISO27001:2013:** A.6.2.2 **NIST800-53 Rev4:** AC-1, AC-4, AC-17, AC-18, PE-17, PL-4, PS-6

Major Control: ACM 4.4 Access Reviews		
ACM 4.4.1	Basic	
Review of User & Accounts Access Rights	Control Type	Technical
Sub-Control	Asset owners should review users' access rights at regular intervals.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The review of access rights should consider the following:

- Users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion, or termination of employment.
- User access rights should be reviewed and re-allocated when moving from one role to another within the same organization.
- Authorizations for privileged access rights should be reviewed at more frequent intervals.
- Privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained.
- Changes to privileged accounts should be logged for periodic review.

Control Reference	**UAE IA:** T5.2.4 **ISO27001:2013:** A.9.2.5 **NIST800-53 Rev4:** AC-2, PE-2 **CIS CSC 7.1**: 3.3

Major Control: ACM 4.5 Network Access Control		
ACM 4.5.1	**Basic**	
Access to Network and Network Services	**Control Type**	**Technical**
Sub-Control	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
A policy should be formulated concerning the use of networks and network services. This policy should cover: • The networks and network services that are allowed to be accessed. • Authorization procedures for determining who is allowed to access which networks and networked services. • Management controls and procedures to protect access to network connections and network services. • The means used to access networks and network services (e.g. use of VPN or wireless network). • User authentication requirements for accessing various network services. • Monitoring of the use of network services.		
Control Reference	**UAE IA:** T5.4.1 **ISO27001:2013:** A.9.1.2 **NIST800-53 Rev4:** AC-1, AC-5, AC-6, AC-17, AC-18, AC-20 **CIS CSC 7.1**: 1.7	
ACM 4.5.2	**Basic**	
Remote User Authentication	**Control Type**	**Technical**
Sub-Control	Remote users should be provided network access through secure channels with appropriate authentication channels by the entity.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
A procedure should be implemented to remotely use of networks and network services and securely authenticating the user, shall include: • The users should access remotely using secure channels such as VPN or encrypted mediums. • The authentication method should be restricted and avoid sharing credentials. • Use of multi-factor authentication for all the remote authentication connections. • Remote user monitoring of network and services access by providing and monitoring granular access.		

Control Reference	**UAE IA:** T5.4.2 **ISO27001:2013:** A.13.1.2 **NIST800-53 Rev4:** CA-3, SA-9 **CIS CSC 7.1**: 9.1	
ACM 4.5.3	Basic	
Equipment Identification	Control Type	**Technical**
Sub-Control	Assets associated with information systems and information processing facilities should be identified, and the inventory should be maintained to avoid unauthorized network access by rogue equipment.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The entity shall implement the procedures to identify the network access such as:

- Maintain authorized equipment inventory connected to the information systems networks.
- Identify unauthorized equipment connected.
- Implement tools to restrict access to information systems networks.

Control Reference	**UAE IA:** T5.4.3 **ISO27001:2013:** A.8.1.1 **NIST800-53 Rev4:** AC-19, IA-3 **CIS CSC 7.1** : 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.4, 15.1, 16.1	
ACM 4.5.4	Organizational	
Remote Diagnostic and Configuration Protection	Control Type	**Technical**
Sub-Control	The controls should be implemented to restricted remote diagnostics and configuration on the authorized information systems by the entity.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The entity shall implement the mechanism such as:

- Monitor the remote administration activities by users and administrators.
- Identify the services required for remote administration, diagnostic and configuration, and restrict access.
- Implement a mechanism for remote diagnostic and configuration to allow on-demand access.
- Restricted access shall allow only authorized accounts, users to perform such tasks.
- Maintain out-of-band access to lower the risk of inaccessibility for disaster recovery.

Control Reference	**UAE IA:** T5.4.4 **ISO27001:2013:** A.13.1.2 **NIST800-53 Rev4:** CA-3, SA-9 **CIS CSC 7.1**: 5.4	
ACM 4.5.5	**Basic**	
Networks Connections Control	**Control Type**	**Technical**
Sub-Control	Access to a private, restricted, and isolated network should be restricted by an entity on a “need to know” basis.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

A policy should be formulated concerning the use of private, restricted, and isolated networks and services. This policy should cover:

- A baseline policy allowing users and applications with least privilege access to private and shared networks.
- A controlled lateral movement to avoid unauthorized access.
- Zero-Trust segmentation to improve the security architecture of individual resources to access or access by other resources, including users, applications, or partners.

Control Reference	**UAE IA:** T5.4.5 **ISO27001:2013:** A.9.1.2 **NIST800-53 Rev4:** AC-3, AC-6, AC-17, AC-18, SC-7 **CIS CSC 7.1**: 1.7	
ACM 4.5.6	**Foundational**	
Networks Routing Control	**Control Type**	**Technical**
Sub-Control	Appropriate network routing controls should be implemented by the entity to ensure un-interrupted information flow, reachability.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The routing controls should be implemented considering business services available to private, restricted, public, and isolated networks and services. This policy should cover:

- Ensure the routing controls are implemented, allowing on-demand access to restricted, isolated, and private information systems.
- Enabling secure routing services on information systems to avoid unauthorized access.
- Implement network segregation using routing controls to enable granular network access for restricted, private, isolated, or public information resources.

- Implement access controls of secure configuration and reviewing of network routing configuration to avoid back-door or errors.
- External network connections must be restricted through network perimeter security controls.
- Peer review of configurations and periodic reviews of routing should be performed to detect and prevent back-doors, unauthorized access, covert channels, or by-pass of defenses

.

Control Reference	**UAE IA:** T5.4.6 **ISO27001:2013:** A.9.1.2 **NIST800-53 Rev4:** AC-4, AC-17, AC-18 **CIS CSC 7.1**: 1.7	
ACM 4.5.7	**Foundational**	
Wireless Access Control	Control Type	**Technical**
Sub-Control	A wireless network must be secured by the entity with appropriate controls to avoid rouge or unauthorized access.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The wireless network should be secured, segregated in line with the access policy. This controls shall cover:

- Ensure that the public and restricted networks are segregated.
- Guest wireless networks should be isolated from the private networks access.
- Restricted wireless networks should not be broadcasted.
- Authentication of the wireless network should inline the authentication policies with strong encryption and keep up to date.
- Ensure the authorization of wireless network access for internal users.
- Configuration of wireless network equipment must be restricted and ensure secure access to the wireless information systems.
- Implement the mechanisms to detect and restrict the unauthorized wireless network equipment to avoid exploitation.

Control Reference	**UAE IA:** T5.4.7 **ISO27001:2013:** A.9.1.2 **NIST800-53 Rev4:** AC-18 **CIS CSC 7.1**: 1.7	
Major Control: ACM 4.6 Operating System Access Control		
ACM 4.6.1	**Basic**	
Secure Log-On Procedures	Control Type	**Technical**

Sub-Control	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

A suitable authentication mechanism should be chosen by the entity to substantiate the claimed identity of the users and applications resources, which shall:

- Not display system or application identifiers until the log-on process has been completed.
- Display a general notice warning that authorized users should only access the computer.
- Not provide help messages during the log-on procedure that would aid an unauthorized user.
- Validate the log-on information only on the completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect.
- Protect against brute force log-on attempts.
- Log unsuccessful and successful attempts.
- Raise a security event if a potential attempted or successful breach of log-on controls is detected
- Display the following information on completion of a successful log-on:
  - Date and time of the previous successful log-on.
  - Details of any unsuccessful log-on attempts since the last successful log-on.
- Not display a password being entered.
- Not transmit passwords in clear text over a network.
- Terminate inactive sessions after a defined period of inactivity, especially in high-risk locations such as public or external areas outside the organization's security management or on mobile devices.
- Restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Control Reference	**UAE IA:** T5.5.1 **ISO27001:2013:** A.9.4.2 **NIST800-53 Rev4:** AC-7, AC-8, AC-9, IA-6 **CIS CSC 7.1** : 4.9, 12.11, 12.12	
ACM 4.6.2	**Basic**	
User Identification and Authentication	**Control Type**	**Technical**
Sub-Control	Identity management of users and application accounts shall be formulated by the entity to provide and monitor activities and prevent usage of shared credentials.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The entity shall implement the mechanism to:

- Provide unique ID Credentials for users and dedicated application accounts.
- Monitor the users and application accounts for login attempts.
- Provide users with required access, preventing excessive privileges.
- Implement network access on a need to know basis using identities.

Control Reference	**UAE IA:** T5.5.2 **ISO27001:2013:** A.9.4.2 **NIST800-53 Rev4:** IA-2, IA-4, IA-5, IA-8 **CIS CSC 7.1** : 4.9, 12.11, 12.12

ACM 4.6.3	**Organizational**	
Use of privileged utility programs	**Control Type**	**Technical**

Sub-Control	The use of utility programs that might be capable of overriding system and application controls should be restricted and firmly controlled.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be considered:

- Use of identification, authentication, and authorization procedures for utility programs.
- Segregation of utility programs from applications software.
- Limitation of the use of utility programs to the minimum practical number of trusted, authorized users.
- Authorization for the ad-hoc use of utility programs.
- Limitation of the availability of utility programs, e.g. for the duration of an authorized change.
- Logging of all use of utility programs.
- Defining and documenting authorization levels for utility programs.
- Removal or disabling of all unnecessary utility programs.
- Not making utility programs available to users who have access to applications on systems where segregation of duties is required.

Control Reference	**UAE IA:** T5.5.4 **ISO27001:2013:** A.9.4.4 **NIST800-53 Rev4:** AC-3, AC-6 **CIS CSC 7.1**: 4.1

Major Control: ACM 4.7 Application and Information Access Control		
ACM 4.7.1	**Basic**	
Information Access Restriction	**Control Type**	**Technical**
Sub-Control	The entity should restrict access to information and application system functions in accordance with the access control policy.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The following should be considered to support access restriction requirements: • Providing menus to control access to application system functions. • Controlling which a particular user can access data. • Controlling the access rights of users, e.g. read, write, delete, and execute. • Controlling the access rights of other applications. • Limiting the information contained in outputs. • Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.		
Control Reference	**UAE IA:** T5.6.1 **ISO27001:2013:** A.9.4.1 **NIST800-53 Rev4:** AC-3, AC-6, AC-14, CM-5 **CIS CSC 7.1**: 14.7	
ACM 4.7.2	**Organizational**	
Sensitive System Isolation	**Control Type**	**Technical**
Sub-Control	The entity shall isolate sensitive systems in a dedicated environment.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
A method of enhancing the security of large networks to divide segregate into separate network segments and domains must be implemented by the entity, which may include: • The segregation for isolated information systems must be based on trust levels • Logical network security can be implemented to access isolated systems. • Perimeters must be defined, and appropriate security controls shall be implemented to isolate information systems. • Authentication and authorization controls should be implemented to access isolated systems to prevent undesired access. • Encrypted connections to isolated systems are desired to prevent certain MIM exploitations.		

Control Reference	**UAE IA:** T5.6.1 **ISO27001:2013:** A.9.4.1 **NIST800-53 Rev4:** AC-3, AC-6, AC-14, CM-5 **CIS CSC 7.1**: 2.1

ACM 4.7.3	**Organizational**	
Publicly Accessible Content	**Control Type**	**Technical**

Sub-Control	The information involved in application services passing over public networks should be protected from fraudulent activity, contract disputes, and unauthorized disclosure and modification.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Information security considerations for application services passing over public networks should include the following:

- The level of confidence each party requires in each other's claimed identity, e.g. through authentication.
- Authorization processes associated with who may approve contents of, issue, or sign key transactional documents.
- Ensuring that communicating partners are fully informed of their authorizations for the provision or use of the service.
- Determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts, e.g. associated with tendering and contract processes.
- The level of trust required in the integrity of key documents.
- The protection requirements of any confidential information.
- The confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts.
- The degree of verification appropriate to verify payment information supplied by a customer.
- Selecting the most appropriate settlement form of payment to guard against fraud.
- The level of protection required to maintain the confidentiality and integrity of order information.
- Avoidance of loss or duplication of transaction information.
- Liability associated with any fraudulent transactions.
- Insurance requirements.

Control Reference	**UAE IA:** T5.6.3 **ISO27001:2013:** A.14.1.2 **NIST800-53 Rev4:** AC-22, SC-14 **CIS CSC 7.1** : 14.6

Major Control: ACM 4.8 Security of Programs Code		
ACM 4.8.1	**Basic**	
Access Control To Program Source Code	**Control Type**	**Technical**
Sub-Control	Access to program source code and associated items should be strictly controlled, to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The following guidelines should then be considered to control access to such program source libraries to reduce the potential for corruption of computer programs: • Where possible, program source libraries should not be held in operational systems. • The program source code and the program source libraries should be managed according to established procedures. • Support personnel should not have unrestricted access to program source libraries. • The updating of program source libraries and associated items and the issuing of program sources to programmers should only be performed after appropriate authorization has been received. • Program listings should be held in a secure environment. • An audit log should be maintained of all accesses to program source libraries. • Maintenance and copying of program source libraries should be subject to strict change control procedures • If the program source code is intended to be published, additional controls to help to get assurance on its integrity (e.g. digital signature) should be considered.		
Control Reference	**UAE IA:** T7.5.3 **ISO27001:2013:** A.9.4.5 **NIST800-53 Rev4:** AC-3, AC-6, CM-5, CM-9, MA-5, SA-10 **CIS CSC 7.1**: 18.7	

5.5. Operations Management

Operations management is considered a crucial element of any business for their continual efforts for business continuity, availability, and sustainability. Healthcare facilities are considered critical to any emerging or existing cybersecurity threats due to the unique nature of information and data being processed by their information systems.

Healthcare facilities ' efforts to improve the cyber-risk posture continuously demand effective Operations Management policies and procedures to be in place to strengthen information handling and protection. The Ministry of Health and Prevention of United Arab Emirates (MOHAP) expects facilities demonstrate commitment by implementing operations security and management controls which may include (but not limited to):

- An Effective Management Policy
- Backup and Archival Procedures
- Vulnerability Management Procedures
- Efficiently Established procedures
- Accountability Procedures
- Malware Prevention Procedures

The common threats posed to any healthcare facility's operations may include:

- Vulnerable Information Systems
- Conceived Operations Planning
- Malware Intrusion
- Unauthorized Changes
- Media Tampering
- Rights Abuse

The objective is to ensure correct and secure operations of information processing facilities, information and information processing facilities are protected against malware, protect against loss of data, record events and generate evidence, prevent exploitation of technical vulnerabilities. The healthcare facility shall consider:

- Effective Operations Planning and Procedures
- Vulnerabilities and Malware Prevention
- Accountability and Archival Management

Major Control: OPM 5.1 Operations Management Policy			
OPM 5.1.1		Basic	
Operations Management Policies		Control Type	**Management**
Sub-Control	The entity must define establish, document ensures correct and secure operations of information processing facilities.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			

The entity must ensure of availability of documented procedures for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, data centers, and mail handling management and safety. The operating procedures should specify the operational instructions, such as:

- The installation and configuration of information systems.
- Processing and handling of information, both automated and manual.
- Backup and secure archival management of the information systems.
- Scheduling requirements, including interdependencies with other systems, earliest job start, and latest job completion times.
- Instructions for handling incidents or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities.
- Support and escalation contacts, including external support contacts in the event of unexpected operational or technical difficulties.
- Special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from unsuccessful jobs.
- System recovery and contingency management procedures for use in the event of system failure.
- The management of audit-trail and system log information.
- Information Systems monitoring procedures to ensure efficient reporting and incident management.

Control Reference	**UAE IA:** T.3.2.2 **ISO27001:2013:** A.12.1.1 **NIST800-53 Rev4:** SA-5

<table>
<tr><th colspan="4">Major Control: OPM 5.2 Planning and Acceptance</th></tr>
<tr><td colspan="2">OPM 5.2.1</td><td colspan="2">Organizational</td></tr>
<tr><td colspan="2"><b>Capacity Management</b></td><td>Control Type</td><td><b>Strategic</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity should monitor and projections should be made to determine the future capacity requirements to ensure the required system performance.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The mechanism must be defined by the entity for the projection of the capacity by monitoring the usage requirements and determining the future requirement with predictions or enhancing the capability of the system by optimizing the information systems resources. The following techniques can be used for optimizing the resources.
• Purging of obsolete data from storage devices.
• Decommissioning of applications, systems, databases, or environments regularly for performance optimization.
• Optimizing batch processes and schedules.
• Optimizing application logic or database queries.
• Denying or restricting bandwidth for resource-hungry services unless business-critical (e.g. video streaming).
• Optimizing operating systems configurations on information systems such as infrastructure equipment.

<b>Strategic Actions</b>: A documented capacity management plan should be crafted for business-critical systems for the projection systems upgrade requirements according to the OEM advisory.</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T3.3.1
<b>ISO27001:2013:</b> A.12.1.3
<b>NIST800-53 Rev4:</b> AU-4, AU-5, CP-2, SA-2, SC-5</td></tr>
<tr><td colspan="2">OPM 5.2.2</td><td colspan="2"><b>Foundational</b></td></tr>
<tr><td colspan="2"><b>System Acceptance and Testing</b></td><td>Control Type</td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity must ensure that new or upgraded information systems are tested against defined, agreed, and documented criteria for acceptance, before becoming operational.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">New information systems, upgrades, and new versions are put through a system acceptance for their acceptability and interoperability. A separate environment comprising of hardware and software is used to carry out tests before deploying or upgrading the main system. Appropriate tests are carried out to confirm that all acceptance criteria are fully satisfied. The test results are documented, and operational, maintenance, and usage procedure are established.</td></tr>
</table>

Training is provided for the use and operation of the new system. Acceptance criteria for new information systems, upgrades, and new versions must be established, and suitable tests of the system carried out before acceptance. • System acceptance process • System acceptance criteria • Security certification • System accreditation	
Control Reference	**UAE IA:** T3.3.2 **ISO27001:2013:** A.14.2.9 **NIST800-53 Rev4:** SA-4, SA-12(7)

Major Control: OPM 5.3 Operational Procedures		
OPM 5.3.1	Basic	
Change Management	Control Type	**Management**
Sub-Control	The entity must ensure a system to document and control the changes to the organization. business processes, information processing facilities, and systems that affect information security.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
In particular, the following items should be considered by the entity: • Identification and recording of significant changes. • Planning and testing of changes • Assessment of the potential impacts, including information security impacts, of such changes. • Formal approval procedure for proposed changes. • Verification that information security requirements have been met. • Communication of change details to all relevant persons. • Fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events. • Provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident.		
Control Reference	**UAE IA:** T3.2.3 **ISO27001:2013:** A.12.1.2 **NIST800-53 Rev4:** CM-3, CM-5, CM-9, SA-10 **CIS CSC 7.1:** 11.3	

OPM 5.3.2	Foundational	
Separation of Test, Development, and Operational Environment	Control Type	**Management**
Sub-Control	The entity should consider separating the development, testing, and operational environments to reduce the risks of unauthorized access or changes to the live operational environment.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The level of separation between operational, testing and development environments that are necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

- Rules for the transfer of software from development to operational status should be defined and documented
- Development and operational software should run on different systems or computer processors and in different domains or directories.
- Changes to operational systems and applications should be tested in a testing or staging environment before being applied to operational systems.
- Other than in exceptional circumstances, testing should not be done on operational systems.
- Compilers, editors, and other development tools or system utilities should not be accessible from operational systems when not required.
- Users should use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error.
- Sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system.

Control Reference	**UAE IA:** T3.2.5 **ISO27001:2013:** A.12.1.4 **NIST800-53 Rev4:** CM-4(1)*, CM-5* **CIS CSC 7.1:** 18.9	
OPM 5.3.3	Foundational	
Software Configuration Restrictions and Baselining	Control Type	**Technical**
Sub-Control	The entity should implement a mechanism to ensure the standard hardening of approved software, implement the standard configuration, and prevent unauthorized installation.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The purpose is to limit the security backdoors/loopholes within the software installed or deployed in the entity information systems by enforcing baseline standard configuration settings across entity's information systems and prevent unauthorized software installation on organizations' information systems.

The following items should be considered:

- Refer to Industry Standards or Frameworks and Best Practices.
- OEM or Vendors recommendations must be followed.
- Proactive Risks mitigation actions such as assessments and audits
- Prevent users from installing unauthorized software.
- Universal Application whitelisting.

Control Reference	**UAE IA:** T3.2.1 **ISO27001:2013:** A.12.6.2 **NIST800-53 Rev4:** CM-5, CM-7(4), CM-7(5), CM-11
OPM 5.3.4	**Foundational**

Segregation of Duties	**Control Type**	**Management**

Sub-Control	The entity should implement policies to prevent any conflict in duties, and areas of responsibilities must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Information Owners must reduce the risk of disruption of information systems by:

- Requiring complete and accurate documentation for every information system.
- Requiring that no single individual has access to all operational functions of an information system (e.g., operating system administrators must not also have application administrator privileges).
- Rotating job duties periodically to reduce the opportunity for single individuals to have sole control and oversight of key systems.
- Requiring that individuals authorized to conduct sensitive operations do not audit the same operations.
- Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action and Implementing security controls to minimize opportunities for collusion.

Control Reference	**UAE IA:** T3.2.4 **ISO27001:2013:** A.6.1.2 **NIST800-53 Rev4:** AC-5

Major Control: OPM 5.4 Malware Protection			
OPM 5.4.1		Basic	
Controls Against Malware		Control Type	Technical
Sub-Control	Detection, prevention, and recovery controls to protect against malware should be implemented by the entity, combined with appropriate user awareness.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			

Protection against malware should be based on malware detection and repair software, information security awareness, and appropriate system access and change management control, such as:

- Establishing a formal policy prohibiting the use of unauthorized software
- Implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting)
- Implementing controls that prevent or detect the use of known or suspected malicious websites by URL filtering. (e.g. blacklisting)
- Establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken.
- Reducing vulnerabilities that could be exploited by malware. e.g. through technical vulnerability management
- Conducting regular reviews of the software and data content of systems supporting critical business processes, the presence of any unapproved files or unauthorized amendments should be formally investigated.
- Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control or on a routine basis.
- Scan any files received over networks or via any form of the storage medium for malware before use.
- Scan email attachments and downloads for malware before use. This scan should be carried out at different places, e.g. at email gateways, email servers, desktop computers, and when entering the network of the organization.
- Scan web pages for malware:
- Defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting, and recovering from malware attacks.
- Preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements,
- Implementing procedures to regularly collect information, such as threat intelligence, URL Blocking feeds by security research organizations.
- Implementing procedures to verify information relating to malware and ensure that warning bulletins are accurate and informative managers should ensure that qualified sources, e.g. reputable journals, reliable internet sites, or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware all users should be made aware of the problem of hoaxes and what to do on receipt of them.
- Isolating environments where catastrophic impacts may result.

Control Reference	**UAE IA:** T3.4.1 **ISO27001:2013:** A.12.2.1 **NIST800-53 Rev4:** AT-2, SI-3, SI-4(24) **CIS CSC 7.1 :** 7.7, 7.10, 8.1, 8.2, 8.4, 8.5, 8.6	
OPM 5.4.2	**Organizational**	
Perimeter Level Malware Protection	**Control Type**	**Technical**
Sub-Control	The deployment malware prevention capability on the external or untrusted network-facing information systems components.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The entity may consider deploying the perimeter level security tools to prevent malware. The following may be considered:

- Deployment of traffic inspection tools to scan malware in inbound and outbound traffic reaching or leaving the entity's information systems, such as emails, web traffic.
- Deployment of technology to prevent access to malicious links by filtering the URLs at the perimeter.

Control Reference	**UAE IA:** T3.4.1 **ISO27001:2013:** A.12.2.1 **NIST800-53 Rev4:** AT-2, SI-3, SI-4(24) **CIS CSC 7.1 :** 7.7, 7.10, 8.1, 8.2, 8.4, 8.5, 8.6

Major Control: OPM 5.5 Backup and Archival		
OPM 5.5.1	**Basic**	
Backup Management	**Control Type**	**Technical**
Sub-Control	Backup copies of information, software, and system images should be taken regularly following the agreed backup policy by the entity.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

A backup policy should be established to define the organization’s requirements for backup of information, software, and systems:

- Accurate and complete records of the backup copies and documented restoration procedures should be produced.
- The extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization.
- Backup media should be regularly tested to ensure that they can‘ be relied upon for emergency use when necessary.
- Testing the ability to restore backed-up data should be performed onto dedicated test media.

Control Reference	**UAE IA:** T3.5.1 **ISO27001:2013:** A.12.3.1 **NIST800-53 Rev4:** CP-9 **CIS CSC 7.1 :** 10.1, 10.3
OPM 5.5.2	**Organizational**

Archived Data Protection	**Control Type**	**Technical**

Sub-Control	The backup policy should define retention and protection requirements. Adequate backup facilities may be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

- The following items should be taken into consideration:
  - The security requirements of the information involved and the criticality of the information to the continued operation of the organization.
  - Backup information should be given an appropriate level of physical and environmental protection.
  - To improve the confidentiality of the critical backed-up information, backups should be protected by means of encryption.

Control Reference	**UAE IA:** T3.5.1 **ISO27001:2013:** A.12.3.1 **NIST800-53 Rev4:** CP-10 **CIS CSC 7.1 :** 10.1, 10.3

Major Control: OPM 5.6 Monitoring and Logging		
OPM 5.6.1	**Basic**	
Monitoring Procedures	**Control Type**	**Management**
Sub-Control	The entity shall introduce the procedures to ensure that all the information systems and applications must be monitored and logged.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity resources of information systems, including the applications, users, and systems monitoring procedures must be established, the procedures such as: • Monitoring of the information system resources for events such as system usage, activities, processing, access, and connections. • Security monitoring procedures must be established, such as data validation, unauthorized access, logs correlation, abnormal activities. • Define the criteria for monitoring the logs to determine the events and incidents. • Establish the roles for monitoring for alerting and escalations.		
Control Reference	**UAE IA:** T3.6.1 **ISO27001:2013:** A.12.4.1 **NIST800-53 Rev4:** AU-3, AU-6, AU-11, AU-12, AU-14 **CIS CSC 7.1 :** 6.2, 8.6, 8.7	
OPM 5.6.2	**Basic**	
Audit Logging	**Control Type**	**Technical**
Sub-Control	The entity shall implement the monitoring procedures by enabling audit logging for information systems.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall enable the logging by (but not limited to): • Determine and identify the functions of the system to monitor information systems, including devices, applications. • Refer to the regulatory, legal, and business requirements to determine the data retention span. • Prevent unauthorized access to the logs data. • Prevent log tempering, modification, or deletion. • Define the SLA to monitor the logs, events, and incidents to prevent escalation.		

Control Reference	**UAE IA:** T3.6.2, T3.6.5, T3.6.6 **ISO27001:2013:** A.12.4.1 **NIST800-53 Rev4:** AU-3, AU-6, AU-11, AU-12, AU-14 **CIS CSC 7.1 :** 6.2, 8.6, 8.7, 8.8	
OPM 5.6.3	**Organizational**	
Preservation of Log Information	**Control Type**	**Technical**
Sub-Control	The entity shall protect the logging facilities and log information against tampering and unauthorized access.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including: • Alterations to the message types that are recorded. • Log files being edited or deleted. • The storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.		
Control Reference	**UAE IA:** T3.6.4 **ISO27001:2013:** A.12.4.2 **NIST800-53 Rev4:** AU-9 **CIS CSC 7.1:** 6.4	
OPM 5.6.4	**Basic**	
Administrators and Operators Logging	**Control Type**	**Technical**
Sub-Control	The entity shall log the system administrator and system operator activities, protect and regularly review the logs.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control; therefore, it is necessary to protect and review the logs to maintain accountability for privileged users. The actions such as below can be taken. • An intrusion detection system managed outside of the control of the system, and network administrators can be used to monitor system and network administration activities for compliance.		
Control Reference	**UAE IA:** T3.6.3 **ISO27001:2013:** A.12.4.3 **NIST800-53 Rev4:** AU-9, AU-12 **CIS CSC 7.1 :** 4.8, 6.7, 14.9	

OPM 5.6.5	**Basic**	
Clock Synchronization	**Control Type**	**Technical**
Sub-Control	The entity’s systems clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
External and internal requirements for time representation, synchronization and accuracy should be documented. Such requirements can be legal, regulatory, contractual requirements, standards compliance, or requirements for internal monitoring. A standard reference time for use within the entity should be defined. The entity’s approach to obtaining a reference time from external sources and how to synchronize internal clocks reliably should be documented and implemented.		
Control Reference	**UAE IA:** T3.6.7 **ISO27001:2013:** A.12.4.4 **NIST800-53 Rev4:** AU-8 **CIS CSC 7.1:** 6.1	

Major Control: OPM 5.7 Security Assessment and Vulnerability Management		
OPM 5.7.1	**Basic**	
Technical Vulnerability Assessment	**Control Type**	**Technical**
Sub-Control	The periodic vulnerability assessment shall be performed by the independent bodies authorized by the entity.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The following should be considered: Periodic assessments for networks, applications, information systems, infrastructure, and security systems such as: ○ Web Applications Penetration testing. ○ Automated Vulnerability Assessment with tools. ○ Penetration testing on network infrastructure and information systems. • Establish a reporting mechanism of the assessment findings to mitigate the vulnerabilities. • Monitor and track the progress of the mitigation actions. • Establish the process for third-party and stakeholders to assess vulnerabilities on the systems before the live usage.		

Control Reference	**UAE IA:** T7.7.1 **ISO27001:2013:** A.12.6.1 **NIST800-53 Rev4:** RA-3, RA-5, SI-2, SI-5 **CIS CSC 7.1:** 3.7	
OPM 5.7.2	**Organizational**	
Preservation and Protection of Assessment Data	**Control Type**	**Technical**
Sub-Control	The entity shall ensure the protection of assessment data for unauthorized access, alterations, or any modifications and preserve in accordance with the data retention policy.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

Controls should aim to protect against unauthorized access to assessment data shall be including:

- The shared reports or data is stored encrypted or transmitted through encrypted communication channels.
- The assessed information systems such as networks, applications, security infrastructure are not being exposed to third-party stakeholders. The assessments being performed on the designated systems and information of any assessment data is being erased from systems after being secured internally.
- Critical information shall not be exposed or available remotely, but only available on the entity’s designated information systems.
- The assessment data is securely stored and available to authorized systems/users.
- The security controls are implemented for the assessment during the retention period until purged or erased.

Control Reference	**UAE IA:** T7.7.1 **ISO27001:2013:** A.12.6.1 **NIST800-53 Rev4:** RA-3, RA-5, SI-2, SI-5 **CIS CSC 7.1:** 3.7

Major Control: OPM 5.8 Audit Controls		
OPM 5.8.1	**Basic**	
Information Systems Audit controls	**Control Type**	**Management**
Sub-Control	The entity shall implement the audit controls involving the verification of operational systems, activities, and be carefully planned to minimize the disruption in business processes.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

- The following guidelines should be observed:
  - Audit requirements for access to systems and data should be agreed with appropriate management.
  - The scope of technical audit tests should be agreed upon and controlled.
  - Audit tests should be limited to read-only access to software and data.
  - Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.
  - Requirements for special or additional processing should be identified and agreed upon.
  - Audit tests that could affect system availability should be run outside business hours.
  - All-access should be monitored and logged to produce a reference trail.

Control Reference	**UAE IA:** M.5.5.1 **ISO27001:2013:** A.12.7.1 **NIST800-53 Rev4:** AU-5* **CIS CSC 7.1:** 8.8

5.6. Communications and Application Security Management

Information systems infrastructure to facilitate the communications and applications delivery is considered the cornerstone of digital transformation, healthcare facilities provide their customers with the state-of-the-art services to improve business agility and patient's convenience with incomparable service delivery and availability. The information processed by healthcare facilities often consists of the most sensitive data, including the Personal Identifiable Information (PII) and Personal Healthcare Information (PHI). It requires the highest level of protection mandated by the decree of law.

The Ministry of Health and Prevention of United Arab Emirates (MOHAP) desires to establish a nation-wide standard framework to be followed to protect such critical information to enhance the healthcare sector's digital security to improve the digital experiences of healthcare users.

Healthcare facilities must establish procedures and implement safeguards to protect the communication, infrastructure, channels, applications, and partners to endow services for information exchange.

The management must establish procedures to proactively implement and enhance the protection parameters and reduce the risk posed to healthcare facility's information exchange channels and critical business supporting applications and continuously improve cybersecurity to mitigate risks and challenges, which may include(but not limited to):

- Communication and Application Security Policies
- Formal Agreement for Information Exchange
- Electronic Commerce Security
- Secure Applications Processing and Delivery
- Secure Information Processing Infrastructure
- Prevention of Unauthorized Access
- Cloud and Information Exchange Platform Security
- Use of Advanced Cryptography

The common threats posed to any healthcare facility's communication infrastructure and business application may include:

- Hacktivism
- Vulnerable Components
- Malicious Code
- Denial of Service
- Eavesdropping
- Unauthorized Access

The objective is to ensure the protection of information in networks, applications, and its supporting information processing facilities, maintain the security of information transferred within an organization, and with any external parties, and ensure that cybersecurity is an integral part of information systems across the entire lifecycle. This also includes the requirements for information applications that provide services over public networks.

Major Control: CAM 6.1 Communications Policy		
CAM 6.1.1	**Basic**	
Communication Policy	**Control Type**	**Management**
Sub-Control	The entity shall develop, document, and publish to organization-defined personnel or roles.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered: • A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls and reviews and updates the current. • System and communications protection policy at organization-defined frequency. • System and communications protection procedures.		
Control Reference	**UAE IA:** T4.1.1 **ISO27001:2013:** A.13.1.1 **NIST800-53 Rev4:** SC-1 **CIS CSC 7.1:** 1.7, 1.8, 7.4, 7.7, 7.9, 9.3, 9.4, 12.2, 12.3, 12.4, 12.6, 12.7, 12.8, 12.9, 13.3, 13.5, 14.2, 14.3, 14.4, 15.2, 15.3, 15.7, 15.8, 16.5	

Major Control: CAM 6.2 Information Exchange			
CAM 6.2.1		**Foundational**	
Information Exchange Procedures		**Control Type**	**Management**
Sub-Control	The entity shall establish formal transfer policies, procedures, and controls should be in place to protect the transfer of information through the use of all types of communication facilities.		

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The procedures and controls to be followed when using communication facilities for information transfer should consider the following items:

- Procedures designed to protect transferred information from interception, copying, modification, misrouting, and destruction.
- Procedures for the detection of and protection against malware that may be transmitted through the use of communications channels.
- Procedures for protecting communicated sensitive electronic information that is in the form of an attachment.
- Policy or guidelines outlining the acceptable use of communication facilities.
- Personnel, external party, and any other user’s responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.
- Use of cryptographic techniques e.g. to protect the confidentiality, integrity, and authenticity of the information.
- Retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations.
- Controls and restrictions associated with using communication facilities, e.g. automatic forwarding of emails to external addresses.
- Advising personnel to take appropriate precautions not to reveal confidential information.

Control Reference		**UAE IA:** T4.2.1 **ISO27001:2013:** A.13.2.1 **NIST800-53 Rev4:** AC-4, AC-20, AC-21, CA-3, PA-4, SC-7, SC-8	
CAM 6.2.2		**Basic**	
Security of Information Transfer		**Control Type**	**Technical**
Sub-Control	The entity shall ensure that critical or confidential information transfer is protected.		

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Any Information may be transferred digitally must address the secure transfer of critical or confidential information within an entity and any external parties. The following may be considered:

- Information transfer agreements may also include the agreed-upon cryptographic standards for encrypting data in transit.
- Use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected.
- Ensuring the prevention of data leakage or loss and responsibilities/liabilities in the event of information security incidents.
- An acceptable level of access control shall be implemented.
- Procedures to ensure traceability and non-repudiation.

Control Reference	**UAE IA:** T4.2.1 **ISO27001:2013:** A.13.2.1 **NIST800-53 Rev4:** AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9	
CAM 6.2.3	**Basic**	
Agreements on Information Transfer	**Control Type**	**Management**

Sub-Control	The entity shall formalize the agreements with third parties and partners to ensure the secure transit of information.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The agreements shall include:

- Management responsibilities for controlling and notifying transmission, dispatch, and receipt of information transfer.
- If the data being transferred is considered HIPAA-protected, then the two parties must enter into a Business Associate Agreement.
- Right to audit and monitor activities that involve PII or PHI of users.
- Establish non-disclosure agreements for all disclosures between the entity and the external parties

Control Reference	**UAE IA:** T4.2.2 **ISO27001:2013:** A.13.2.2 **NIST800-53 Rev4:** CA-3, SA-9	
CAM 6.2.4	**Foundational**	
Security Awareness for Partners and Third Parties	**Control Type**	**Management**

Sub-Control	The entity shall educate the partners and third parties of the security requirements of information exchange and transfer.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The awareness agreements shall include:

- Policies, procedures, and standards to protect information and physical media and should be documented in agreements and formally agreed upon, ensuring the parties' awareness.

Control Reference	**UAE IA:** T4.2.2 **ISO27001:2013:** A.13.2.2 **NIST800-53 Rev4:** CA-3, SA-9
CAM 6.2.5	**Foundational**

Physical Media in Transit	**Control Type**	**Technical**

Sub-Control	The entity shall ensure the protection of information carried upon physical media while in transit.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The entity shall formalize the policy and implement, such as:

- Maintaining a chain of custody and tracking for information while in transit.
- Any special controls that are required to protect sensitive information from:
  - Disclosure
  - Loss or destruction of media.
  - Tempering or Alteration of Media
- Use of trusted courier service for secure transportation of media.

Control Reference	**UAE IA:** T4.2.3 **ISO27001:2013:** A.13.2.1 **NIST800-53 Rev4:** MP-5
CAM 6.2.6	**Basic**

Electronic Messaging	**Control Type**	**Technical**

Sub-Control	The entity shall implement appropriate security controls to protect the information exchange via electronic messaging.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Information security considerations for electronic messaging should include the following:

- Protecting messages from unauthorized access, modification, or denial of service commensurate with the classification scheme adopted by the organization.
- Ensuring correct addressing and transportation of the message.
- Reliability and availability of the service.
- Legal considerations, for example, requirements for electronic signatures.
- Obtaining approval before using external public services such as instant messaging, social networking, or file-sharing.
- Stronger levels of authentication controlling access from publicly accessible networks.

Control Reference	**UAE IA:** T4.2.4 **ISO27001:2013:** A.13.2.3 **NIST800-53 Rev4:** SC-8 **CIS CSC 7.1 :** 7.8, 13.4
CAM 6.2.7	**Organizational**

Business Information System Security	**Control Type**	**Technical**

Sub-Control	The entity shall secure the information exchange through the application services using integrated business networks from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

Information security considerations should include the following:

- Identification of the information passing through the integrated connection and implement the suitable security controls accordingly.
- Classify and Prioritize the information based on criticality to determine the security controls.

Control Reference	**UAE IA:** T4.2.5 **ISO27001:2013:** A.14.1.2 **NIST800-53 Rev4:** CA-1, CA-3

<table>
<tr><th colspan="3">Major Control: CAM 6.3 Electronic Commerce</th></tr>
<tr><td><b>CAM 6.3.1</b></td><td colspan="2"><b>Foundational</b></td></tr>
<tr><td><b>Security of Electronic Commerce Services</b></td><td><b>Control Type</b></td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="2">The entity shall implement security controls to protect the information passing over the public or external networks.</td></tr>
<tr><td colspan="3">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="3">The controls to be implemented to protect the electronic commerce information being transferred, the entity should consider the following items:
• Maintain a service catalogue of all the electronic commerce services.
• Define the security baseline controls and agree with partners to build upon.
• Identify the information type and flow end to end to be able to implement the agreed security controls.</td></tr>
<tr><td><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> T4.3.1
<b>ISO27001:2013:</b> A.14.1.2
<b>NIST800-53 Rev4:</b> AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14
<b>CIS CSC 7.1:</b> 18.10</td></tr>
<tr><td><b>CAM 6.3.2</b></td><td colspan="2"><b>Foundational</b></td></tr>
<tr><td><b>Security of Public Services and Information</b></td><td><b>Control Type</b></td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="2">The entity shall protect the information systems and services available through public networks.</td></tr>
<tr><td colspan="3">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="3">The controls to be implemented to secure the information systems and service available through the public networks, the entity should consider the following items:
• Identify the services and information systems available through public networks.
• Ensure the integrity of the information and services available through public networks.
• Ensure the information or services has been reviewed and approved before being published on public networks.
• Maintain the availability of the information systems and the published information by preventing any denial of access.
• Authorization processes associated with who may approve the publishing of the services or information publicly.</td></tr>
</table>

Control Reference	**UAE IA:** T4.3.3 **ISO27001:2013:** A.14.1.2 **NIST800-53 Rev4:** SC-14 **CIS CSC 7.1 :** 9.5, 18.10	
CAM 6.3.3	**Foundational**	
Digital Transactions	Control Type	**Technical**
Sub-Control	The entity shall protect the Information involved in application service transactions to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

Information security considerations for digital transactions should include the following:

- The use of electronic signatures by each of the parties involved in the transaction.
- Ensure that the user’s secret authentication information of all parties is valid and verified.
- The transaction remains confidential.
- Privacy associated with all parties involved is retained
- The communications path between all involved parties is encrypted.
- Protocols used to communicate between all involved parties are secured.
- Where a trusted authority is used, such as the purposes of issuing and maintaining digital signatures or digital certificates, security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

Control Reference	**UAE IA:** T4.3.2 **ISO27001:2013:** A.14.1.3 **NIST800-53 Rev4:** SC-3, SC-7, SC-8, SC-9, SC-14 **CIS CSC 7.1 :** 9.5, 18.10

Major Control: CAM 6.4 Network Security Management		
CAM 6.4.1	Basic	
Network Controls	Control Type	Technical
Sub-Control	The entity should manage and control the networks to protect the information in systems and the applications.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall implement the security controls to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items may be considered: • Responsibilities and procedures for the management of networking equipment should be established. • Operational responsibility for networks should be separated from computer operations where appropriate. • Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or wireless networks and to protect the connected systems and applications, special controls may also be required to maintain the availability of the network services and computers connected. • Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. • Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure. • Systems on the network should be authenticated. • Systems connected to the network should be authorized and restricted.		
Control Reference	**UAE IA:** T4.5.1 **ISO27001:2013:** A.13.1.1 **NIST800-53 Rev4:** AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23 **CIS CSC 7.1 :** 1.7, 1.8, 7.4, 7.7, 7.9, 9.3, 9.4, 12.2, 12.3, 12.4, 12.6, 12.7, 12.8, 12.9, 13.3, 13.5, 14.2, 14.3, 14.4, 15.2, 15.3, 15.7, 15.8, 16.5	
CAM 6.4.2	Foundational	
Security of Network Services	Control Type	Technical
Sub-Control	The entity shall identify and develop a security mechanism to secure the network services whether provided on-prem or outsourced.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall develop an ability to manage the network services or maintain the service level agreements to		

manage services securely:

- Identify the network services to define the service level agreements for each service depends on the risk posture.
- Establish security baseline requirements for implements.
- Ensure the right to audit in SLAs to assess the network services against the network baseline controls.

Control Reference	**UAE IA:** T4.5.2 **ISO27001:2013:** A.13.1.2 **NIST800-53 Rev4:** SA-9, SC-8, SC-9 **CIS CSC 7.1:** 9.1	
CAM 6.4.3	Basic	
Networks Segregation	Control Type	**Technical**
Sub-Control	The entity shall segregate network information services, users, and information systems.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The entity shall segregate physical, logical, and wireless networks based on criticality, nature of services, and users information systems such as:

- Establish criteria for network segregation
- Establish and maintain appropriate network security zones, allowing data flow to follow through a controlled path
- Establish minimum and specific security requirements for each of the segregated networks, zones, and resources
- Periodically evaluate the adequacy of implemented segregation strategy

Control Reference	**UAE IA:** T4.5.3 **ISO27001:2013:** A.13.1.3 **NIST800-53 Rev4:** AC-4, SA-8, SC-7 **CIS CSC 7.1 :** 9.2, 11.7, 14.1, 15.10	
CAM 6.4.4	Basic	
Wireless Networks	Control Type	**Technical**
Sub-Control	The entity shall ensure that all wireless networks are protected with adequate controls.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The security controls should be implemented, such as:

- Identify secure physical locations to install wireless access points to avoid unnecessary wireless links/signal exposure.
- Use strong and updated wireless encryptions for authentication and data flow.
- Implement the authorization controls to prevent unauthorized access to wireless networks.
- Segregate the untrusted wireless networks from secure/trusted, such as guest networks and enterprise wireless networks.

Control Reference	**UAE IA:** T4.5.4 **ISO27001:2013:** A.13.1.2 **NIST800-53 Rev4:** AC-4, SA-8, SC-7 **CIS CSC 7.1:** 9.1

Major Control: CAM 6.5 Information Systems and Application Security		
CAM 6.5.1	Foundational	
Information Security Requirements Analysis and Specification	Control Type	Management
Sub-Control	The entity shall ensure that security requirements are established and functionally integrated into information systems.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The controls shall include:

- The level of confidence required towards the claimed identity of users, to derive user authentication requirements.
- Access provisioning and authorization processes, for business users as well as for privileged or technical users.
- Informing users and operators of their duties and responsibilities.
- The required protection needs of the assets involved, regarding availability, confidentiality, integrity.
- Requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements.
- Requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems.

Control Reference	**UAE IA:** T7.2.1 **ISO27001:2013:** A.14.1.1 **NIST800-53 Rev4:** SA-1, SA-3, SA-4

Major Control: CAM 6.6 Secure & Accurate Processing in Applications			
CAM 6.6.1		Foundational	
Input Data Validation		Control Type	Technical
Sub-Control	The entity shall implement suitable controls to validate data input to applications to ensure that this data is correct and appropriate.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
The controls may include: • Define a set of guidelines or parameters to be used to validate data input into applications • Define a set of values for each guideline or parameter to identify acceptable and unacceptable values • Provide guidance on how to validate each guideline or parameter			
Control Reference		**UAE IA:** T7.3.1 **ISO27001:2013:** A.14.2.5 **NIST800-53 Rev4:** SI-9, SI-10 **CIS CSC 7.1:** 5.1	
CAM 6.6.2		Foundational	
Output Data Validation		Control Type	Technical
Sub-Control	The entity shall implement suitable controls to validate output data from applications to ensure the accuracy of data.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
The controls may include: • Plausibility checks to test whether the output data is reasonable • Reconciliation control counts to ensure processing of all data • Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information • Procedures for responding to output validation tests • Creating a log of activities in the data output validation process			
Control Reference		**UAE IA:** T7.3.4 **ISO27001:2013:** A.14.2.5 **NIST800-53 Rev4:** SI-15 **CIS CSC 7.1:** 5.1	

CAM 6.6.3	Foundational	
Internal Processing Capabilities	Control Type	Technical
Sub-Control	The entity shall incorporate validation checks into applications to detect any corruption of information through processing errors or deliberate acts.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The controls may include: • The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimized. • An appropriate checklist should be prepared, activities documented, and the results should be kept secure. Examples of checks that can be incorporated. • Periodically review existing applications to ensure validation checks included during their development still met minimum requirements. • Provide guidelines to application developers on minimum requirements for validation checks for applications under development.		
Control Reference	**UAE IA:** T7.3.2 **ISO27001:2013:** A.14.2.8 **NIST800-53 Rev4:** SI-7, SI-9, SI-10	
CAM 6.6.4	Foundational	
Message Integrity	Control Type	Technical
Sub-Control	The entity shall ensure the authenticity, integrity, and non-repudiation of messages in applications.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The controls may include: • Identify requirements to ensure the authenticity and integrity of messages transmitted between systems and applications • Proper technical countermeasures should be adopted to ensure the integrity of messages during transmissions such as hashing or digital signatures.		
Control Reference	**UAE IA:** T7.3.3 **ISO27001:2013:** A.14.2.5 **NIST800-53 Rev4:** AU-10, SC-8, SI-7 **CIS CSC 7.1:** 5.1	
CAM 6.6.5	Foundational	

Fault Tolerance and Continuity	**Control Type**	**Technical**
Sub-Control	The entity shall ensure the functionality and ability of applications to function offline.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall add the capabilities in the application, such as: • Offline and/or out-of-sequence response message handling capabilities to tolerate communication failure.		
Control Reference	**UAE IA:** T7.3.2 **ISO27001:2013:** A.14.2.5 **NIST800-53 Rev4:** SI-7, SI-9, SI-10 **CIS CSC 7.1:** 5.1	

<table>
<tr><th colspan="4">Major Control: CAM 6.7 Cryptography</th></tr>
<tr><td colspan="2">CAM 6.7.1</td><td colspan="2">Foundational</td></tr>
<tr><td colspan="2"><b>Management Policy for Cryptographic Controls</b></td><td>Control Type</td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity shall develop and implement a policy on the use of cryptographic controls for information protection.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The management policy may include:
• The management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected
• Identify the risk to determine the required encryption method and strength appropriate to the application.
• Key management processes such as key protections, contingency planning due to loss or compromise of keys.
• Use of encryption for the data in transit such as communication channels for web or mobile applications.</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T7.4.1
<b>ISO27001:2013:</b> A.10.1.1
<b>NIST800-53 Rev4:</b> SC-12
<b>CIS CSC 7.1 :</b> 13.9, 14.4, 14.8, 15.7, 16.4, 16.5, 18.5</td></tr>
<tr><td colspan="2">CAM 6.7.2</td><td colspan="2">Foundational</td></tr>
<tr><td colspan="2"><b>Cryptographic Key Management</b></td><td>Control Type</td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity shall establish key management to support the entity's use of cryptographic techniques.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The key management process may include and consider:
All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store, and archive keys should be physically protected.
• Generating keys for different cryptographic systems and different applications
• Generating and obtaining public key certificates
• Distributing keys to intended users including how keys should be activated when received
• Storing keys including how authorized users obtain access to keys
• Changing or updating keys including rules on when keys should be changed and how this will be done</td></tr>
</table>

- Revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an entity (in which case keys should also be archived) - Recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information - Archiving keys, e.g. for information archived or backed up - Logging and auditing of key management related activities	
Control Reference	**UAE IA:** T7.4.2 **ISO27001:2013:** A.10.1.2 **CIS CSC 7.1 :** 13.5, 13.6

Major Control: CAM 6.8 Security of System Files		
CAM 6.8.1	Organizational	
Software Installation on Live Systems	Control Type	**Technical**
Sub-Control	The entity shall develop and implement procedures to control the installation of software on live/operational systems.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The following guidelines should be considered to control changes in software on operational systems: - Trained administrators should only perform the updating of the operational software, applications, and program libraries upon appropriate management authorization. - Operational systems should only hold approved executable code and nondevelopment code or compilers. - Applications and operating system software should only be implemented after extensive and successful testing. the tests should cover usability, security, effects on other systems, and user-friendliness and should be carried out on separate systems it should be ensured that all corresponding program source libraries have been updated - A configuration control system should be used to keep control of all implemented software as well as the system documentation. - A rollback strategy should be in place before changes are implemented. - An audit log should be maintained of all updates to operational program libraries. - Previous versions of application software should be retained as a contingency measure. - Old versions of the software should be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data are retained in the archive.		

Control Reference	**UAE IA:** T7.5.1 **ISO27001:2013:** A.12.5.1 **NIST800-53 Rev4:** CM-3, CM-5, CM-7(4), CM-7(5), CM-11 **CIS CSC 7.1 :** 2.6	
CAM 6.8.2	**Foundational**	
Protection of System Test Data	**Control Type**	**Technical**
Sub-Control	The entity shall select test data carefully, protect, and control unauthorized access. If any confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The following guidelines should be applied to protect operational data when used for testing purposes: • The access control procedures, which apply to operational application systems, should also apply to test application systems. • There should be separate authorization each time operational information is copied to a test environment. • Operational information should be erased from a test environment immediately after the testing is complete. • The copying and use of operational information should be logged to provide an audit trail.		
Control Reference	**UAE IA:** T7.5.2 **ISO27001:2013:** A.14.3.1 **NIST800-53 Rev4:** SA-3(2)*, AC-3, AC-4	

Major Control: CAM 6.9 Outsourced Software Development		
CAM 6.9.1	**Foundational**	
Outsourced Software Development	Control Type	**Technical**

Sub-Control	The entity shall develop and implement procedures to supervise and monitor the activity of outsourced system development.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

When system development is outsourced, the following points should be considered across the organization's entire external supply chain:

- Licensing arrangements, code ownership, and intellectual property rights related to the outsourced content.
- Contractual requirements for secure design, coding, and testing practices.
- Provision of the approved threat model to the external developer.
- Acceptance testing for the quality and accuracy of the deliverables.
- Provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality.
- Provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery.
- Provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities.
- Escrow arrangements, e.g. if source code is no longer available.
- Contractual right to audit development processes and controls.
- Effective documentation of the built environment used to create deliverables.
- The entity remains responsible for compliance with applicable laws and control efficiency verification.

Control Reference	**UAE IA:** T7.6.5 **ISO27001:2013:** A.14.2.7 **NIST800-53 Rev4:** SA-1, SA-4, SA-6, SA-7, SA-8, SA-9, SA-11, SA-12, SA-13 **CIS CSC 7.1:** 18.1

<table>
<tr><th colspan="4">Major Control: CAM 6.10 Non-Disclosure and Confidentiality</th></tr>
<tr><td colspan="2">**CAM 6.10.1**</td><td colspan="2">**Foundational**</td></tr>
<tr><td colspan="2">**Non-Disclosure and Confidentiality**</td><td>**Control Type**</td><td>**Management**</td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity shall establish requirements for confidentiality or Non- Disclosure Agreements reflecting the entity’s needs for the protection of information.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The following should be considered:
• Define a Non-Disclosure Agreement (NDA) template to be used to legally protect confidential information and ownership of information
• Have an information classification process in place to identify which information is subject to the terms of the NDA
• Keep a track record of all signed NDAs and perform a periodical review</td></tr>
<tr><td colspan="2">**Control Reference**</td><td colspan="2">**UAE IA:** M.1.3.2
ISO27001:2013: A.13.2.4
NIST800-53 Rev4: PS-6</td></tr>
</table>

5.7. Healthcare Information Security

The healthcare sector has major reliance on the information processing facilities to provide agility to provide services to the customers by processing, maintaining, and storing Patient Health Information(PHI) which is by law and ethical business practices is a fundamental right of patients and individuals must be protected. Health information systems are business-critical and demand higher levels of protection is connected environments.

Healthcare entities shall establish procedures to protect the information processing facilities, data, and medical equipment to prevent any security breaches to enhance public trust. It is mandated by the Ministry of Health and Prevention of United Arab Emirates (MOHAP) that the Health information must be highly classified and protected throughout the lifecycle and the medical equipment must be access controlled to avoid any unauthorized or illegal access.

The motive of Healthcare information security shall be, but not limited to:

- Establishing SOPs of Access Management
- Prevention of Unauthorized Access
- Prevention of alteration of Information
- PHI Data Leakage or Loss
- Security of Medical Equipment
- Classification of Healthcare Assets

The common threats posed any healthcare entity with PHI can be:

- PHI Data Leakage or Loss
- Data Forging
- Privacy Breach
- Unauthorized Access
- Abuse of Access
- Misuse of Clinical Data

The objective is to ensure the healthcare information (PHI) must be protected along with any information related to Personal Identifiable Information (PII) should be considered highly classified and dealt accordingly to enhance the public trust in healthcare facilities. MOHAP interests and reputation must prevail.

<table>
<tr><th colspan="4">Major Control: HIS 7.1 Health Information Protection Policy</th></tr>
<tr><td colspan="2">HIS 7.1.1</td><td colspan="2">Basic</td></tr>
<tr><td colspan="2">**Health Information Protection Policy**</td><td>Control Type</td><td>**Management**</td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity shall develop, enforce and maintain a health information protection policy that ensures management’s commitment to protect healthcare information</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The management policy must:
• Define management requirements on;
o Criteria for access and acceptable usage
o Accountability and/or data ownership
o Healthcare data communication or sharing
• Mandate the requirements of non-disclosure and confidentiality during and after employment
• Define government sanctions and legal obligations
• Include reference to the organizational disciplinary process</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2">**UAE IA:** M5.2.4
ISO27001:2013: A.5.1.1
NIST800-53 Rev4: PL-5; SI-12</td></tr>
</table>

Major Control: HIS 7.2 Health Information Privacy and Protection		
HIS7.2.1	Basic	
Security of Healthcare Information	Control Type	**Management**
Sub-Control	The entity shall ensure that healthcare information under its custody is suitably protected.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
• Conduct orientation on healthcare information protection and sanctions to all its employees, relevant contractors, and third parties before their access to healthcare information • Establish a stricter process to ensure clear desk and clear screen practices are adhered to in areas where healthcare information is used, processed, or handled • Define and enforce criteria for healthcare information access • Ensure access to health information systems and applications are restricted for individuals possessing a valid license to practice their profession within the UAE, and any exception shall be authorized by entity CISO based on adequate justification • Control and restrict privileges for printing and sharing of healthcare information • Ensure cleaning staff access to areas where patient-related healthcare information is being viewed, accessed, used, processed, stored, and/or destroyed are monitored or under surveillance coverage • Ensure any hardcopy/media containing healthcare information is shredded after its usefulness • Establish processes for shredding all hardcopy documents before their disposal • Ensure that healthcare information with personal identifiers is not available unattended • Ensure the printing of healthcare information is limited to local printers and are not printed through uncontrolled network printers • Establish processes to notify the health sector regulator of any probabilities of breaches involving healthcare information		
Control Reference	**UAE IA:** M5.2.4 **ISO27001:2013:** A.18.1.4 **NIST800-53 Rev4:** PL-5; SI-12	

Major Control: HIS 7.3 Medical Asset Handling		
HIS7.3.1	Basic	
Medical Devices Management Procedures	**Control Type**	**Technical**
Sub-Control	The healthcare entity shall establish medical devices and equipment management procedures for each category of identified medical devices and equipment.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The management policy must: • The healthcare entity shall establish medical devices and equipment management procedures for each category of identified medical devices and equipment.		
Control Reference	**UAE IA:** T3.2.2 **ISO27001:2013:** A.12.1.1 **NIST800-53 Rev4:** AC-19, IA-3	
HIS7.3.2	Basic	
Access Allocation for Medical Devices	**Control Type**	**Technical**
Sub-Control	Access and privilege allocation for medical devices shall be provided to defined roles, with essential qualifications and experience required to operate.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The healthcare entity shall: • Secure and safeguard medical devices and equipment in accordance with its classification scheme and risk factor		
Control Reference	**UAE IA:** T5.4.1 **ISO27001:2013:** A.9.1.2 **NIST800-53 Rev4:** AC-6 **CIS CSC 7.1:** 1.7	
HIS7.3.3	**Foundational**	
Security of Information within Medical Devices	**Control Type**	**Technical**

<table>
<tr><td>Sub-Control</td><td colspan="3">The healthcare entity shall prevent unauthorized disclosure, modification, destruction, or loss of patient health information stored on medical devices and equipment.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">It must be ensured that,
• Information stored within the medical devices and equipment shall be encrypted
• Electronic communication between medical devices and equipment shall be encrypted
• Healthcare entities shall define the minimum essential qualification required to operate and/or handle medical devices and equipment
• Copies of valuable health data are moved to a secure storage/location to reduce the risk of its data damage or loss</td></tr>
<tr><td colspan="2"><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> T7.3.2
<b>ISO27001:2013:</b> A.14.2.8
<b>NIST800-53 Rev4:</b> N/A
<b>CIS CSC 7.1 :</b> 2.5</td></tr>
<tr><td colspan="2"><b>HIS7.3.4</b></td><td colspan="2"><b>Foundational</b></td></tr>
<tr><td colspan="2"><b>Communication Facility for Medical Devices</b></td><td><b>Control Type</b></td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">Healthcare facilities shall consider wired communication facilities for medical devices and equipment. The usage of wireless communication facilities with medical devices and equipment shall be avoided to the extent possible.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">Healthcare facilities shall consider wired communication facilities for medical devices and equipment. The usage of wireless communication facilities with medical devices and equipment shall be avoided to the extent possible.</td></tr>
<tr><td colspan="2"><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> T5.7.1
<b>ISO27001:2013:</b> A.6.2.1
<b>NIST800-53 Rev4:</b> N/A
<b>CIS CSC 7.1 :</b> 13.6</td></tr>
</table>

<table>
<tr><th colspan="3">Major Control: HIS 7.4 Medical Equipment and Devices Access Control</th></tr>
<tr><td>HIS7.4.1</td><td colspan="2">Foundational</td></tr>
<tr><td><b>Access Control for Portable and Medical Devices</b></td><td><b>Control Type</b></td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="2">The healthcare entity shall protect confidential and secret information on portable or removable media, mobile or portable devices, and medical equipment or devices.</td></tr>
<tr><td colspan="3">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="3">The healthcare entity shall:
• Authenticate user, where relevant, access to equipment, devices, and media
• Ensure media containing confidential and secret information is password protected and encrypted
• Where relevant, control access to medical equipment and devices through password enforcement in compliance with the healthcare entities password complexity and usage requirements
Control access to mobile and portable devices hosting confidential and secret information
• Establish mobile device management process to protect entity information being used, processed, or stored in mobile devices</td></tr>
<tr><td><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> T5.7.1
<b>ISO27001:2013:</b> A.6.2.1
<b>NIST800-53 Rev4:</b> AC-1, AC-17, AC-18, AC-19, PL-4, PS-6
<b>CIS CSC 7.1 :</b> 13.6</td></tr>
</table>

5.8. Third Parties and Supply Chain Management

In a fast-paced, dynamic healthcare business environment the facilities rely excessively on third parties services to provide numerous services and support services delivery which includes resources, operations support whereas the suppliers have become an essential part of the business to fulfil certain requirements to improve and enhance business capabilities. The suppliers and third-parties involvement in the modern healthcare business are nearly ineluctable and require robust security measures to prevent unfortunate security incidents.

The Ministry of Health and Prevention of United Arab Emirates (MOHAP) and Healthcare facilities are aware that any information or data being processed externally outside the secure perimeter of the entity may be exposed to various threats regardless of the sensitivity of information or valuably crucial.
A portion of breaches and threats originates from entrusted “Blind-spots” which may impair reputation, public trust and cause monetary damages.

Effective due-diligence measures taken by management to mitigate such threats can improve the risk posture of a facility by establishing a security framework which may include:

- Management Compliance Policy
- Privilege Management
- Contingency Planning
- Service Level Expectation & Agreements
- Third-Party Audits
- Accountability and Monitoring

The common threats posed to any healthcare facility’s supply chain or by entrusted parties may include:

- Disclosure of Sensitive Data/Information
- Interrupted Supply Chain
- Breach of Contractual Relations
- Illegal or Unauthorized Access
- Violation of SLAs
- Vulnerable B2B Assets

The objective is to ensure the protection of the organization’s assets that is accessible, maintain an agreed level of information security and service delivery in line with supplier agreements with suppliers and third parties.

Major Control: TSM 8.1 Security Policy for Supply Chain and Third-Parties Management			
TSM 8.1.1		Basic	
Security Policy for Supply Chain and Third-Parties Management		Control Type	**Management**
Sub-Control	A management security policy must be developed by the entity, addressing the third parties and Suppliers' security.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
The management policy must facilitate the implementation of the associated controls and to reduce probabilities of risk realization concerning third parties and supplier organizations. Covers aspects such as: • Relevancy with Suppliers and Third-Party Relations with Entity. • Secure management of Third parties and suppliers for services covering Information Security Objectives. • Defining the responsibilities of Suppliers and Third Parties. • Business Requirements concerning Information security aspects. • Management expectations on the privacy and protection of information assets. • Secure access to applications, assets, and resources mutually. • Non-disclosure, terms, and acceptability of usage. • Formally signed and agreed by the stakeholders, third parties, and suppliers.			
Control Reference	**UAE IA:** T6.1.1 **ISO27001:2013:** A.15.1.1 **NIST800-53 Rev4:** PS-7		

Major Control: TSM 8.2 Third-Party Service Delivery and Monitoring		
TSM 8.2.1	Basic	
Secure Third-Party Service Agreements	Control Type	Management
Sub-Control	The entity must establish the requirements and agree with each third-party and supplier that may access, process, store, communicate, or provide components for, the organization's information.	

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The management should establish the agreements document to ensure that there is no misunderstanding between the organization and the third-party/supplier regarding both parties' obligations to fulfil relevant information security requirements.

- Description of the information to be provided or accessed and methods of providing or accessing the information.
- Classification of information according to the organization's classification scheme if necessary, also mapping between the organization's classification scheme and the classification scheme of the third-party/supplier.
- Legal and regulatory requirements, including data protection, intellectual property rights, and copyright, and a description of how it will be ensured that they are met.
- The obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting, and auditing.
- Rules of acceptable use of information, including unacceptable use if necessary.
- Either an explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel.
- Information security policies are relevant to the specific contract.
- Incident management requirements and procedures (especially notification and collaboration during incident remediation).
- Training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures.
- Relevant regulations for sub-contracting, including the controls that need to be implemented.
- Relevant agreement partners, including a contact person for information security issues.
- Screening requirements, if any, for supplier's personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern.
- The right to audit the Third-party/supplier processes and controls related to the agreement.
- Reflect resolution and conflict resolution processes.
- Third-party/supplier obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report.
- Third-party/supplier obligations to comply with the organization's security requirements.

Control Reference	**UAE IA:** T6.2.1 **ISO27001:2013:** A.15.1.2 **NIST800-53 Rev4:** SA-9

<table>
<tr><td colspan="2"><b>TSM 8.2.2</b></td><td colspan="2"><b>Foundational</b></td></tr>
<tr><td colspan="2"><b>Monitoring and Review of Third-Party Services</b></td><td><b>Control Type</b></td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity must establish monitoring capabilities to monitor, report, and record the third-party services.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The monitoring and review of the services must include:
• Information security compliance in the contracts, agreements with third parties.
• Monitoring of the services to ensure the reporting by an entity.
• Perform the third-party information security audits to ensure compliance.
• Implement security controls to ensure secure information exchange between entities and third parties, monitor access to avoid incidents or violations of access.
• Assessment of the contracts to identify and mitigate the commercial, financial risks involved.</td></tr>
<tr><td colspan="2"><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> T6.2.2
<b>ISO27001:2013:</b> A.15.2.1
<b>NIST800-53 Rev4:</b> SA-9</td></tr>
<tr><td colspan="2"><b>TSM 8.2.3</b></td><td colspan="2"><b>Foundational</b></td></tr>
<tr><td colspan="2"><b>Managing Changes to Third Party Services</b></td><td><b>Control Type</b></td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">Management procedures must be established by the entity to manage and formalize changes in third-party services.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The management process to manage changes and formalization must include:
• Compliance requirements met and security controls are implemented as per the business regulation requirements.
• Change descriptions must be defined and communicated as per the defined parameters by the entity and third-party.
• The established procedures must be part of the communications and agreements of changes between an entity and a third-party.</td></tr>
<tr><td colspan="2"><b>Control Reference</b></td><td colspan="2"><b>UAE IA:</b> T6.2.3
<b>ISO27001:2013:</b> A.15.2.2
<b>NIST800-53 Rev4:</b> RA-3, SA-9</td></tr>
<tr><td colspan="4"><b>Major Control: TSM 8.3 Information Systems Acquisition, Development, and Maintenance Policy</b></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
</table>

TSM 8.3.1	Basic	
Information Systems Acquisition, Development and Maintenance Policy	Control Type	**Management**

Sub-Control	A management policy must be established and enforced for information systems acquisition, development, and maintenance to facilitate the implementation of secure development and maintenance practices.

IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)

The management policy for the information systems acquisition, development and maintenance must cover the aspects below:

- Be relevant and appropriate to the model and relationship of the entity and involved internal and external stakeholders
- Demonstrate management’s commitment, objectives, and directions
- Establish a framework that facilitates:
- Defining and including information security objectives
- Selection of the right model and approach
- Identification and mitigation of risks in involved business and application processes
- Definition of roles and responsibilities

Establish management expectations on:

- Privacy and protection of information assets
- Secure design, development, testing, deployment, maintenance, and support
- Secure access to systems, applications, devices, and equipment
- Secure processing and communication of information and data
- Non-disclosures requirements
- Cryptographic controls and requirements
- Be read and acknowledged by involved internal and external stakeholders

Control Reference	**UAE IA:** T7.1.1, T7.4.1 **ISO27001:2013:** A.10.1.1, A.14.2.1 **NIST800-53 Rev4:** SA-1, MA-1, SI-1 IA-7, SC-8, SC-9, SC-12, SC-13 **CIS CSC 7.1 :** 13.9, 14.4, 14.8, 15.7, 16.4, 16.5, 18.1, 18.5

Major Control: TSM 8.4 Supply Chain Management		
TSM 8.4.1	Organizational	
Supplier Reviews	Control Type	Management
Sub-Control	The entity should regularly monitor, review, and audit supplier service delivery.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The management should ensure the Monitoring and review of supplier services information security terms and conditions of the agreements are being adhered to, and that information security incident and problems are managed properly. This should involve a service management relationship process between the organization and the supplier to: • Monitor service performance levels to verify adherence to the agreements. • Review service reports produced by the supplier and arrange regular progress meetings as required by the agreements. • Conduct audits of suppliers, in conjunction with a review of independent auditor's reports, if available, and follow-up on issues identified. • Provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures. • Review supplier audit trails and records of information security events, operational problems, failures, tracing of faults, and disruptions related to the service delivered. • Resolve and manage any identified problems. • Review information security aspects of the supplier's relationships with its suppliers. • Ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.		
Control Reference	**UAE IA:** T7.8.2 **ISO27001:2013:** A.15.2.1 **NIST800-53 Rev4:** SA-12	
TSM 8.4.2	Organizational	
Secure Supply Chain Operations	Control Type	Technical
Sub-Control	The entity shall implement appropriate security controls to ensure secure supply chain operations.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

<table>
<tr><td colspan="4">Supply chain information can include the user identities, uses for information systems, information system components, information system services, supplier identities, supplier processes. The entity must fulfil the security requirements such as:
• Evaluate potential risks to its information systems and services considering threats & vulnerabilities related to suppliers.
• Map threats in the contract term with the suppliers and propose appropriate security controls to mitigate the threats.
• Define the procedures to monitor the security control implemented by the supplier.</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T7.8.4
<b>ISO27001:2013:</b> A.15.2.2
<b>NIST800-53 Rev4:</b> SA-12</td></tr>
<tr><td colspan="2">TSM 8.4.3</td><td colspan="2">Organizational</td></tr>
<tr><td colspan="2"><b>Reliable Delivery of Items and Services</b></td><td>Control Type</td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity shall establish the process to maintain the reliable delivery of information systems components, hardware, and services.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The process must be established by the entity to monitor and ensure the reliability of the deliverables, which may include the deliverables such as:
• The authenticity of information systems components, such as hardware, licenses.
• The authenticity of software code, ensuring no alterations or back doors.</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T7.8.4
<b>ISO27001:2013:</b> A.15.2.2
<b>NIST800-53 Rev4:</b> SA-12</td></tr>
<tr><td colspan="2">TSM 8.4.4</td><td colspan="2">Foundational</td></tr>
<tr><td colspan="2"><b>Contingency Planning of Critical Supplies</b></td><td>Control Type</td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">The entity shall plan and establish the processes to maintain continuity of critical supplies for information systems.</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
</table>

<table>
<tr><td colspan="2">The process must be established by the entity to monitor and ensure the reliability of the deliverables, which may include the deliverables such as:

The entity must establish contingency procedures to maintain supplies for critical information systems components and support, which can include actions such as:

• Maintain redundant inventory of critical components.
• Establish relations with multiple suppliers to ensure the availability of supplies.
• Introduce terms in the contracts for contingency situations to ensure the SLAs are fulfilled.</td></tr>
<tr><td><b>Control Reference</b></td><td><b>UAE IA:</b> T7.8.6
<b>ISO27001:2013:</b> A.15.2.1
<b>NIST800-53 Rev4:</b> SA-14</td></tr>
</table>

5.9. Security Incident Management

The complexity of information processing systems and healthcare sector reliance on universal connectivity, complex applications, and expanded infrastructures makes them vulnerable to targeted threats of cybercriminals and makes cybersecurity incidents inevitable. It demands effective incident management planning which includes important aspects of detecting, reporting, and responding to adverse security events/incidents as well as weaknesses which may lead to events if they are not appropriately addressed.

Though the management running information security programs are aware that the incidents are not completely preventable, but implementing the appropriate controls and enhancing capability can improve the risk posture and ability to deal with residue effectively by minimizing the frequency or severity of the security incident occurred to disrupt the information systems at any healthcare entity by communicating with authorities or incident response management organizations at an early stage.

The motive of developing an effective Security Incident Management Program for Cybersecurity should be, but not limited to:

- Incident Response Procedures
- Incident Classification Mechanism
- Effective Communication Channels with Authorities
- Effective Incident Response Team
- Discovering the Weaknesses
- Incident Recovering Procedures.

The Information Security Incidents may cause the breaches of critical business functions, which may include threats such as:

- Denial of Service
- Privilege Escalation
- Unauthorized Access
- Information Loss or Leakage
- Malware or Ransomware Attacks
- Covert Channels

The objective is to define suitable processes to ensure the Information and cybersecurity incident is detected, responded mitigated in timely manners, minimize the impact, and effective restoration mechanism for healthcare entities. The process may include:

- Incident Management Policing
- Incident Response Procedures
- Weaknesses Reporting and Recovery Procedures

<table>
<tr><th colspan="4">Major Control: SIM 9.1 Information Security Incident Policy</th></tr>
<tr><td colspan="2">SIM9.1.1</td><td colspan="2">Basic</td></tr>
<tr><td colspan="2"><b>Information Security Incident Management Policy</b></td><td>Control Type</td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="3">An entity shall develop, enforce and maintain a cybersecurity incident management policy, to manage and guide the entity’s response to incidents</td></tr>
<tr><td colspan="4">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="4">The policy shall:
• Be relevant and appropriate to the entity’s operation and risk environment
• Demonstrate management commitment, objectives, and directions
• Establish incident management roles and responsibilities
• Establish a proactive, collaborative, and sustainable process of identifying and resolving adverse information security incidents.
• Establish management demands on:
○ Incident identification
○ Incident response
○ Incident notification/communication
○ Learning from incident
• Be read and acknowledged by involved internal and external stakeholders</td></tr>
<tr><td colspan="2">Control Reference</td><td colspan="2"><b>UAE IA:</b> T8.1.1
<b>ISO27001:2013:</b> A.16.1.1
<b>NIST800-53 Rev4:</b> IR-1
<b>CIS CSC 7.1:</b> 19.1</td></tr>
</table>

<table>
<tr><th colspan="3">Major Control: SIM 9.2 Incident Management and Improvements</th></tr>
<tr><td>SIM 9.2.1</td><td colspan="2">Foundational</td></tr>
<tr><td><b>Incident Response Procedures</b></td><td>Control Type</td><td><b>Management</b></td></tr>
<tr><td>Sub-Control</td><td colspan="2">The entity shall establish a Computer Security Incident Response Team (CSIRT) responsible for incident management and response efforts.</td></tr>
<tr><td colspan="3">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="3">The process(es) shall:
• Have tested procedures to handle incident situations before, during, and after the occurrence of the incident
• Plan for incident communication to affected stakeholders and relevant authorities
• Management approval on plans and procedures</td></tr>
<tr><td>Control Reference</td><td colspan="2"><b>UAE IA:</b> T8.2.1
<b>ISO27001:2013:</b> A.16.1.1
<b>NIST800-53 Rev4:</b> IR-8
<b>CIS CSC 7.1:</b> 19.1</td></tr>
<tr><td>SIM 9.2.2</td><td colspan="2">Organizational</td></tr>
<tr><td><b>Incident Response Team Responsibilities</b></td><td>Control Type</td><td><b>Technical</b></td></tr>
<tr><td>Sub-Control</td><td colspan="2">Ownership for each identified asset shall be assigned to a designated role</td></tr>
<tr><td colspan="3">IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)</td></tr>
<tr><td colspan="3">The entity shall:
• Establish CSIRT organization with adequate authority, essential roles, and responsibilities
• Identify and nominate competent resources for each identified role of the CSIRT
• Establish communication and response protocols
• Allocate adequate funds for CSIRT operations
• Entity CSIRT shall coordinate with its counterparts within the health sector regulator of UAE for incidents which will have a significant/severe impact on the entity’s assets or operations
• Ensure that significant/severe impact incidents are reported to the health sector regulator of UAE
• Provide suitable training to members of the CSIRT to cover:
○ Past incidents and lessons learned
○ Current threat environment of the entity
○ New threats and attack trends across the world</td></tr>
</table>

Control Reference	**UAE IA:** T8.2.2 **ISO27001:2013:** A.16.1.1 **NIST800-53 Rev4:** IR-10 **CIS CSC 7.1:** 19.1	
SIM 9.2.3	**Foundational**	
Security Incident Assessment and Classification	Control Type	**Technical**
Sub-Control	The entity shall assess and classify information security incidents	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall: • Establish an incident classification scheme in line with the recommendations of the health sector regulator of UAE. • Define workflows to handle incidents of various classifications/severity		
Control Reference	**UAE IA:** T8.2.3 **ISO27001:2013:** A.16.1.4 **NIST800-53 Rev4:** AU-6, IR-4 **CIS CSC 7.1:** 19.8	
SIM 9.2.4	**Foundational**	
Response to Information Security Incidents	Control Type	**Technical**
Sub-Control	The entity must respond to information security incidents in accordance with the documented procedures.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Information Security Incidents should be responded by a nominated point of contact and other relevant persons of the organization or external parties. This should include; • collecting evidence as soon as possible after the occurrence, • conducting information security forensics analysis, as required, • escalation, as required, • ensuring that all involved response activities are properly logged for later analysis, • communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know, • dealing with information security weakness(es) found to cause or contribute to the incident, • once the incident has been successfully dealt with, formally closing and recording it,		

- Post-incident analysis should take place, as necessary, to identify the source of the incident.

Control Reference	**UAE IA:** T8.2.5 **ISO27001:2013:** A.16.1.5 **NIST800-53 Rev4:** IR-3	
SIM 9.2.5	**Foundational**	
Incident Evidence Collection	Control Type	**Technical**
Sub-Control	The entity should define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The Entity should develop and follow the procedures when dealing with the evidence for disciplinary and legal action. In general, these procedures for evidence should provide processes of identification, collection, acquisition, and preservation of evidence in accordance with different types of media, devices, and status of devices, e.g. powered on or off. The procedures should take account of;

- chain of custody,
- safety of evidence,
- safety of personnel,
- roles and responsibilities of personnel involved,
- competency of personnel,
- documentation,
- briefing.

Control Reference	**UAE IA:** T8.2.7, T8.2.9 **ISO27001:2013:** A.16.1.7 **NIST800-53 Rev4:** AU-9, IR-4	
SIM 9.2.6	**Organizational**	
Learning from Incidents	Control Type	**Technical**
Sub-Control	The entity should use the knowledge gained from analyzing and resolving information security incidents to reduce the likelihood or impact of future incidents.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The entity should develop mechanisms to enable the types, volumes, and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents. The Entity shall consider measures such as (but not limited to): • The number of detected but unsuccessful intrusion attempts to compare with the number of successful ones • The damage/losses caused by disruptive incidents, to help develop plans for reducing outages and the staff hours spent responding to incidents • Reductions in downtime of the network or critical systems • Metrics for any special security initiatives such as alarms or monitoring of systems, to help in assessing their effectiveness	
Control Reference	**UAE IA:** T8.2.4, T8.2.8 **ISO27001:2013:** A.16.1.6 **NIST800-53 Rev4:** IR-2, IR-4

Major Control: SIM 9.3 Information Security Events and Weakness Reporting		
SIM 9.3.1	Organizational	
Reporting Information Security Events	Control Type	**Management**
Sub-Control	The entity shall report Information security events through appropriate management channels.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
Information Security Incident should also be made aware of the information security events, and the point of contact should be provided to the employees and the team to which the events should be reported. Situations to be considered for information security event reporting such as; • ineffective security control, • breach of information integrity, confidentiality, or availability expectations, • human errors, • non-compliances with policies or guidelines, • breaches of physical security arrangements, • uncontrolled system changes, • malfunctions of software or hardware, • Access violations.		
Control Reference	**UAE IA:** T8.3.2 **ISO27001:2013:** A.16.1.2 **NIST800-53 Rev4:** AU-6, IR-1, IR-6, SI-4, SI-5 **CIS CSC 7.1 :** 19.5	
SIM 9.3.2	Organizational	

Reporting Security Weakness		Control Type	Technical
Sub-Control	The entity must make the employees and contractors awar7e of information security to report any suspected information security weakness/es.		
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)			
The entity must run campaigns to make employees and contractors aware who should report these matters to the information security team or Incident management team as quickly as possible to prevent information security incidents. The reporting mechanism should be as easy, accessible, and available as possible, such as: • Helpline • Email Distribution List			
Control Reference		**UAE IA:** T8.3.3 **ISO27001:2013:** A.16.1.3 **NIST800-53 Rev4:** PL-4, SI-2, SI-4, SI-5 **CIS CSC 7.1 :** 19.4	

5.10. Information Systems Continuity Management

While business in the healthcare sector increases dependency on the information systems and application to perform the critical business operations, it has become heavily vulnerable to the disruption caused by discontinuity on systems. Recognizing that not all events can be prevented, and some risks may be deemed acceptable, proper planning is essential to maintain or restore services when an unexpected or unavoidable event disrupts normal operations.

Business continuity planning includes the identification of vulnerabilities, priorities, dependencies, and measures for developing plans to facilitate continuity and recovery before, during, and after such a disruption. Comprehensive business continuity plans are designed and implemented to ensure continuity of operations under abnormal conditions.

Plans are based on a risk assessment and business impact analysis and include a process for regular maintenance, which may include:

- Business Continuity Planning
- Continuity Risk Management
- Disaster Recovery Planning
- Testing and Drills

The common threats posed to a healthcare entity which may disrupt critical business functions:

- Denial of Service
- Equipment Failure
- Destruction of Facility or Media
- System Failure/Malfunction
- Accidents
- Power Failures

The objective is to ensure that the business in the healthcare sector develops and adhere to the systems continuity plans to eliminate, minimize or transfer the impact on information systems, applications and resources during the abnormal operating conditions, which may include:

- Information Systems Continuity Planning
- Disaster Recovery Planning and Testing

Major Control: SCM 10.1 Information Systems Continuity Management Policy		
SCM 10.1.1	Foundational	
Information Systems Continuity Management Policy	**Control Type**	**Management**
Sub-Control	The entity must develop, enforce, and maintain an information system continuity planning policy as per the business requirements to manage risks that challenge the continuous availability of information systems and applications supporting critical business services.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The management policy must: • Be relevant and appropriate to the business's information systems and applications continuity demands • Demonstrate strategic planning, objectives, and directives and initiatives. • Establish roles and responsibilities of involved stakeholders, including departments, vendors, and partners. • Establish management expectations on: ○ Planning for information system and application continuity during adverse situations ○ Compliance with organizational business continuity plans ○ Testing of continuity and restoration plans • Be read and acknowledged by involved internal and external stakeholders organizational disciplinary process		
Control Reference	**UAE IA:** T9.1.1 **ISO27001:2013:** A.17.1.1 **NIST800-53 Rev4:** CP-1	

Major Control: SCM 10.2 Information Systems Continuity Planning		
SCM 10.2.1	Organizational	
Developing Information System and Application Continuity Plans	**Control Type**	**Strategic**
Sub-Control	The entity shall develop information systems and application continuity plans that shall prevent or minimize interruptions to critical business services and processes during adverse situations.	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The plan shall:

- Identify information systems, processes, and information supporting critical business services and processes
- Be harmonized and support organizational business continuity planning and/or disaster recovery demands
- Identify individuals with assigned roles and responsibilities, along with necessary contact information
- Define call tree matrix and escalation matrix
- Defined criteria and conditions for plan activation
- Have provisions to address information security incident-based scenarios and provide guidance to operate and support critical business services during such scenarios

Control Reference	**UAE IA:** T9.2.1 **ISO27001:2013:** A.17.1.2 **NIST800-53 Rev4:** CP-2	
SCM 10.2.2	Organizational	
Implementing Information System and Application Continuity Plans	**Control Type**	**Technical**
Sub-Control	The entity shall implement the established information system and application continuity plans	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		

The entity shall:

- Ensure that the capabilities and requirements of the information system and application continuity plans are established and available to be used during plan activation

Control Reference	**UAE IA:** T9.2.2 **ISO27001:2013:** A.17.1.3 **NIST800-53 Rev4:** CP-2

	CIS CSC 7.1 : 10.2	
SCM 10.2.3	Organizational	
Testing, Maintaining, and Reassessing Plans	**Control Type**	**Technical**
Sub-Control	The entity shall test, reassess and maintain its information systems and application continuity plans	
IMPLEMENTATION GUIDANCE (FOR INFORMATION PURPOSE ONLY)		
The entity shall: • Define schedules and test information system and application continuity plan to ensure: ○ Adequacy and effectiveness of the plans ○ Entity and resource readiness to execute the plans • Document test outcomes and lessons learned • Assess plan adequacy during changes to business services, systems, and applications • Update and maintain information system and application continuity plans based on lessons learned and assessment outcome		
Control Reference	**UAE IA:** T9.3.1 **ISO27001:2013:** A.17.2.1 **NIST800-53 Rev4:** CP-4, CP-5	

6. SECTION – 3

This section will provide a summary for the document with appendixes, references, and controls mapping tables.

- Summary of Domains and Controls
- Summary of Major Controls and Sub-Controls
- Appendix
- References

6.1. Summary of Domains & Controls

The Riayati Information and Cyber Security Standard are divided into 10 Security Domains and 51 Major Controls and 140 subsequent sub-controls listed in a table below.

Domain #	Domain Name	Domain Alias	# of Major Control	# of Sub-Controls
1	Human Resource Security	HRS	4	11
2	Asset Management	ASM	5	14
3	Physical and Environmental Security	PHE	3	18
4	Access Control Management	ACM	8	22
5	Operations Management	OPM	8	19
6	Communications and Applications Security Management	CAM	10	27
7	Healthcare Information Security	HIS	4	7
8	Third Parties and Supply Chain Management	TSM	4	9
9	Security Incident Management	SIM	3	9
10	Information Systems Continuity Management	SCM	2	4

6.2. Summary of Major Controls and Sub-Controls

The Riayati ICS Standard’s ten domains are divided into 51 Major Controls, and 140 subsequent sub-controls, controls criteria, and controls are summarized below.

Reference	Control Name	Control Type	Control Criteria
HRS 1.1: Human Resources Security Policy			
HRS1.1.1	Human Resource Security Policy	Management	Basic
HRS 1.2: Prior to the Employment			
HRS1.2.1	Background Verification Check	Management	Basic
HRS1.2.2	Terms and Condition of Employment	Management	Basic
HRS 1.3: During Employment			
HRS1.3.1	Compliance to Organizational Policies and Procedures	Management	Basic
HRS1.3.2	Cybersecurity Training	Technical	Basic
HRS1.3.3	Awareness Campaign	Management	Basic
HRS1.3.4	Disciplinary Process	Management	Foundational
HRS 1.4: Termination or Change of Employment and Role			
HRS1.4.1	Termination Responsibility	Management	Basic
HRS1.4.2	Return of Assets	Management	Basic
HRS1.4.3	Removal of Access Rights	Technical	Basic
HRS1.4.4	Internal Transfers and Change Of Role	Technical	Basic
ASM 1.1: Asset Management Policy			
ASM2.1.1	Asset Management Policy	**Management**	**Basic**
ASM 2.2: Management of Asset			
ASM2.2.1	**Asset Inventory**	**Technical**	**Basic**
ASM2.2.2	Asset Ownership	Management	Basic
ASM2.2.3	Usage Acceptability of Assets	Management	Basic
ASM2.2.4	Acceptable Bring Your Own Device Arrangements	Technical	Basic
ASM 2.3 : Asset Classification & Labelling			
ASM2.3.1	Information Classification and Re-Classification	Management	Basic
ASM2.3.2	Information Valuation, Protection, and Classification Schema	Technical	Foundational
ASM2.3.3	Asset Labeling	Technical	Basic
ASM 2.4: Asset Handling			

ASM2.4.1	Asset Handling Procedures	Technical	Basic
ASM2.4.2	Management of Removable Media	Technical	Basic
ASM2.4.3	Removal and Movement of Information Assets	Technical	Foundational
ASM 2.5: Asset Disposal			
ASM2.5.1	Secure Information Asset or Media Disposal	Technical	Basic
ASM2.5.2	Procedures for Re-Use of Assets	Management	Foundational
ASM2.5.3	Records on Disposal	Management	Organizational
Domain 3: Physical and Environmental Security			
PHE 3.1: Physical and Environmental Security Policy			
PHE3.1.1	Management Policy for Physical and Environmental Security	Management	Basic
PHE 3.2: Secure or Restricted Areas			
PHE3.2.1	Physical Security Perimeter	Technical	Basic
PHE3.2.2	Secure Areas Control Measures	Technical	Foundational
PHE3.2.3	Secure Office & Meeting Rooms	Technical	Basic
PHE3.2.4	Protection against External & Environmental Threats	Technical	Basic
PHE3.2.5	Effectiveness of Control Measures	Management	Foundational
PHE3.2.6	Working in Secure Areas	Management	Basic
PHE3.2.7	Physical Security Awareness	Management	Foundational
PHE3.2.8	Delivery and Loading Areas	Management	Basic
PHE 3.3: Equipment Security			
PHE3.3.1	Equipment siting and protection	Technical	Basic
PHE3.3.2	Supporting Utilities	Technical	Foundational
PHE3.3.3	Cabling Security	Technical	Basic
PHE3.3.4	Equipment Maintenance	Technical	Organizational
PHE3.3.5	Removal of Equipment	Technical	Foundational
PHE3.3.6	Security of Equipment Off-premises	Technical	Organizational
PHE3.3.7	Secure disposal or re-use of equipment	Technical	Foundational
PHE3.3.8	Unattended User Equipment	Technical	Basic
PHE3.3.9	Clear Desk & Clear Screen Policy	Technical	Basic
[redacted]			
ACM 4.1: Access Control Policy			
ACM4.1.1	Access Control Policy	Management	Basic
ACM 4.2: User Access Management			
ACM4.2.1	User Registration and De-Registration	Technical	Basic
ACM4.2.2	Privilege Management	Technical	Organizational
ACM4.2.3	Use and Management of Security Credential	Technical	Basic

ACM4.2.4	Use of secret authentication information	Technical	Basic
ACM4.2.5	Password management system	Technical	Basic
ACM 4.3: Equipment and Devices Access Control			
ACM4.3.1	Access Control for Assets and Equipment in Teleworking Sites	Technical	Foundational
ACM 4.4: Access Reviews			
ACM4.4.1	Review of User & Accounts Access Rights	Technical	Basic
ACM 4.5: Network Access Control			
ACM4.5.1	Access to Network and Network Services	Technical	Basic
ACM4.5.2	Remote User Authentication	Technical	Basic
ACM4.5.3	Equipment Identification	Technical	Basic
ACM4.5.4	Remote Diagnostic and Configuration Protection	Technical	Organizational
ACM4.5.5	Networks Connections Control	Technical	Basic
ACM4.5.6	Networks Routing Control	Technical	Foundational
ACM4.5.7	Wireless Access Control	Technical	Foundational
ACM 4.6: Operating System Access Control			
ACM4.6.1	Secure Log-On Procedures	Technical	Basic
ACM4.6.2	User Identification and Authentication	Technical	Basic
ACM4.6.3	Use of privileged utility programs	Technical	Organizational
ACM 4.7: Application and Information Access Control			
ACM4.7.1	Information Access Restriction	Technical	Basic
ACM4.7.2	Sensitive System Isolation	Technical	Organizational
ACM4.7.3	Publicly Accessible Content	Technical	Organizational
ACM 4.8: Security of Programs Code			
ACM4.8.1	Access Control To Program Source Code	Technical	Basic
OPM 5.1: Operations Management Policy			
OPM5.1.1	Operations Management Policies	Management	Basic
OPM 5.2: Planning and Acceptance			
OPM5.2.1	Capacity Management	Strategic	Organizational
OPM5.2.2	System Acceptance and Testing	Technical	Foundational
OPM 5.3: Operational Procedures			
OPM5.3.1	Change Management	Management	Basic
OPM5.3.2	Separation of Test, Development, and Operational Environment	Management	Foundational
OPM5.3.3	Software Configuration Restrictions and Baselining	Technical	Foundational
OPM5.3.4	Segregation of Duties	Management	Foundational
OPM 5.4: Malware Protection			
OPM5.4.1	Controls Against Malware	Technical	Basic

OPM5.4.2	Perimeter Level Malware Protection	Technical	Organizational
OPM 5.5: Backup and Archival			
OPM5.5.1	Backup Management	Technical	Basic
OPM5.5.2	Archived Data Protection	Technical	Organizational
OPM 5.6: Monitoring and Logging			
OPM5.6.1	Monitoring Procedures	Management	Basic
OPM5.6.2	Audit Logging	Technical	Basic
OPM5.6.3	Preservation of Log Information	Technical	Organizational
OPM5.6.4	Administrators and Operators Logging	Technical	Basic
OPM5.6.5	Clock Synchronization	Technical	Basic
OPM 5.7: Security Assessment and Vulnerability Management			
OPM5.7.1	Technical Vulnerability Assessment	Technical	Basic
OPM5.7.2	Preservation and Protection of Assessment Data	Technical	Organizational
OPM 5.8: Audit Controls			
OPM5.8.1	Information Systems Audit controls	Management	Basic
CAM 6.1: Communications Policy			
CAM6.1.1	Communication Policy	Management	Basic
CAM 6.2: Information Exchange			
CAM6.2.1	Information Exchange Procedures	Management	Foundational
CAM6.2.2	Security of Information Transfer	Technical	Basic
CAM6.2.3	Agreements on Information Transfer	Management	Basic
CAM6.2.4	Security Awareness for Partners and Third Parties	Management	Foundational
CAM6.2.5	Physical Media in Transit	Technical	Foundational
CAM6.2.6	Electronic Messaging	Technical	Basic
CAM6.2.7	Business Information System Security	Technical	Organizational
CAM 6.3: Electronic Commerce			
CAM6.3.1	Security of Electronic Commerce Services	Technical	Foundational
CAM6.3.2	Security of Public Services and Information	Technical	Foundational
CAM6.3.3	Digital Transactions	Technical	Foundational
CAM 6.4: Network Security Management			
CAM6.4.1	Network Controls	Technical	Basic
CAM6.4.2	Security of Network Services	Technical	Foundational
CAM6.4.3	Networks Segregation	Technical	Basic
CAM6.4.4	Wireless Networks	Technical	Basic
CAM 6.5: Information Systems and Application Security			
CAM6.5.1	Information Security Requirements Analysis and Specification	Management	Foundational
CAM 6.6: Secure & Accurate Processing in Applications			
CAM6.6.1	Input Data Validation	Technical	Foundational

CAM6.6.2	Output Data Validation	Technical	Foundational
CAM6.6.3	Internal Processing Capabilities	Technical	Foundational
CAM6.6.4	Message Integrity	Technical	Foundational
CAM6.6.5	Fault Tolerance and Continuity	Technical	Foundational
CAM 6.7: Cryptography			
CAM6.7.1	Management Policy for Cryptographic Controls	Management	Foundational
CAM6.7.2	Cryptographic Key Management	Technical	Foundational
CAM 6.8: Security of System Files			
CAM6.8.1	Software Installation on Live Systems	Technical	Organizational
CAM6.8.2	Protection of System Test Data	Technical	Foundational
CAM 6.9: Outsourced Software Development			
CAM6.9.1	Outsourced Software Development	Technical	Foundational
CAM 6.10: Non-Disclosure and Confidentiality			
CAM6.10.1	Non-Disclosure and Confidentiality	Management	Foundational
HIS 7.1: Health Information Protection Policy			
HIS7.1.1	Health Information Protection Policy	Management	Basic
HIS 7.2: Health Information Privacy and Protection			
HIS7.2.1	Security of Healthcare Information	Management	Basic
HIS 7.3: Medical Asset Handling			
HIS7.3.1	Medical Devices Management Procedures	Technical	Basic
HIS7.3.2	Access Allocation for Medical Devices	Technical	Basic
HIS7.3.3	Security of Information within Medical Devices	Technical	Foundational
HIS7.3.4	Communication Facility for Medical Devices	Technical	Foundational
HIS 7.4: Medical Equipment and Devices Access Control			
HIS7.4.1	Access Control for Portable and Medical Devices	Technical	Foundational
TSM 8.1: Security Policy for Supply Chain and Third-Parties Management			
TSM8.1.1	Security Policy for Supply Chain and Third-Parties Management	Management	Basic
TSM 8.2: Third-Party Service Delivery and Monitoring			
TSM8.2.1	Secure Third-Party Service Agreements	Management	Basic
TSM8.2.2	Monitoring and Review of Third-Party Services	Management	Foundational
TSM8.2.3	Managing Changes to Third Party Services	Management	Foundational
TSM 8.3: Information Systems Acquisition, Development, and Maintenance Policy			
TSM8.3.1	Information Systems Acquisition, Development and Maintenance Policy	Management	Basic

TSM 8.4: Supply Chain Management			
TSM8.4.1	Supplier Reviews	Management	Organizational
TSM8.4.2	Secure Supply Chain Operations	Technical	Organizational
TSM8.4.3	Reliable Delivery of Items and Services	Technical	Organizational
TSM8.4.4	Contingency Planning of Critical Supplies	Management	Foundational
SIM 9.1: Information Security Incident Policy			
SIM9.1.1	Information Security Incident Management Policy	Management	Basic
SIM 9.2: Incident Management and Improvements			
SIM9.2.1	Incident Response Procedures	Management	Foundational
SIM9.2.2	Incident Response Team Responsibilities	Technical	Organizational
SIM9.2.3	Security Incident Assessment and Classification	Technical	Foundational
SIM9.2.4	Response to Information Security Incidents	Technical	Foundational
SIM9.2.5	Incident Evidence Collection	Technical	Foundational
SIM9.2.6	Learning from Incidents	Technical	Organizational
SIM 9.3: Information Security Events and Weakness Reporting			
SIM9.3.1	Reporting Information Security Events	Management	Organizational
SIM9.3.2	Reporting Security Weakness	Technical	Organizational
SCM 10.1: Information Systems Continuity Management Policy			
SCM10.1.1	Information Systems Continuity Management Policy	Management	Foundational
SCM 10.2: Information Systems Continuity Planning			
SCM10.2.1	Developing Information System and Application Continuity Plans	Strategic	Organizational
SCM10.2.2	Implementing Information System and Application Continuity Plans	Technical	Organizational
SCM10.2.3	Testing, Maintaining and Reassessing Plans	Technical	Organizational

6.3. Appendix

Appendix 1. Compliance Matrix for Smaller Entities

The following controls are applicable for smaller entities

Applicable Controls for Smaller Entities		Criteria
HRS1.1.1	Security Aspects of Employment and Termination	Basic
HRS1.2.1	Background Verification Check	Basic
HRS1.2.2	Terms and Condition of Employment	Basic
HRS1.4.1	Termination Responsibility	Basic
HRS1.4.2	Return of Assets	Basic
HRS1.4.3	Removal of Access Rights	Basic
HRS1.4.4	Internal Transfers and Change Of Role	Basic
PHE3.3.1	Equipment Siting and Protection	Basic
PHE3.3.6	Unattended User Equipment	Basic
ACM4.2.1	User Registration and De-Registration	Basic
ACM4.4.1	Review of User Access Rights	Basic
ACM4.6.2	User Identification and Authentication	Basic
ACM4.7.1	Information Access Restriction	Basic
OPM5.4.1	Controls Against Malware	Basic
HIS7.2.1	Security of Healthcare Information	Basic
HIS7.3.2	Access Allocation for Medical Devices	Basic
PHE3.3.9	Clear Desk & Clear Screen Policy	Basic

Appendix 2: Riayati ICS Mapping Against Leading Standards

The tables below provide the list of the Riayati Standard’s Control mapping against the Nationally and Internationally recognized Information and Cyber Security Standards and Frameworks such as UAE Information Assurance Framework(UAE IA), ISO27001:2013, NIST Special Publication 800-53 Revision 4, SANS Center of Internet Security (CIS) Critical Security Controls Top 20 Version 7.1.

This mapping enables the participating entities to compare the requirements of the UAE IA Standards against other leading standards.

Control Ref.	Control Name	UAE IA	ISO27001:2013	NIST 800-53	CIS 7.1
1. Human Resource Security					
HRS1.1.1	Human Resource Security Policy	M3.1.1, M4.1.1	A.6.1.1	PS-1	-
HRS1.2.1	Background Verification Check	M4.2.1	A.7.1.1	PS-3	-
HRS1.2.2	Terms and Condition of Employment	M4.2.2	A.7.1.2	AC-20, PL-4, PS-6, PS-7	-
HRS1.3.1	Compliance to Organizational Policies and Procedures	M4.3.1	A.18.2.2	PL-4, PS-6, PS-7, SA-9	-
HRS1.3.2	Cybersecurity Training	M3.2.1, M3.3.3, M3.3.4,	A.7.2.2	AT-3	17.2, 17.3, 17.4, 17.5,

		M3.3.5 M3.3.1, M3.3.2			17.6, 17.7, 17.8. 17.9
HRS1.3.3	Awareness Campaign	M3.4.1	A.7.2.2	AT-3	17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8. 17.9
HRS1.3.4	Disciplinary Process	M3.4.2	A.7.2.3	PS-8	-
HRS1.4.1	Termination Responsibility	M4.4.1	A.7.3.1	PS-4, PS-5	16.8, 16.9
HRS1.4.2	Return of Assets	M4.4.2	A.8.1.4	PS-4, PS-5	1.6
HRS1.4.3	Removal of Access Rights	M4.4.3	A.9.2.1	AC-2, PS-4, PS-5	16.6
HRS1.4.4	Internal Transfers and Change Of Role	M4.4.3	A.9.2.1	AC-2, PS-4, PS-5	16.6
2. Asset Management					
ASM2.1.1	Asset Management Policy	T.1.1.1	A.8.1.1	MP-1, CM-1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.4, 15.1, 16.1
ASM2.2.1	Asset Inventory	T.1.2.1	A.8.1.1	CM-8, CM-9, PM-5	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.4, 15.1, 16.1
ASM2.2.2	Asset Ownership	T.1.2.2	A.8.1.2	CM-8, CM-9, PM-5	1.5
ASM2.2.3	Usage Acceptability of Assets	T.1.2.3	A.8.1.3	AC-20, PL-4	5.1, 7.1, 15.4, 15.5, 15.6, 15.9, 16.11
ASM2.2.4	Acceptable Bring Your Own Device Arrangements	T.1.2.4	A.6.2.1	IA-8, AC-20	13.6
ASM2.3.1	Information Classification and Re-Classification	T.1.3.1	A.8.2.1	RA-2	13.1
ASM2.3.2	Information Valuation, Protection and Classification Schema	T.1.3.1	A.8.2.1	RA-2	13.1
ASM2.3.3	Asset Labeling	T.1.3.2	A.8.2.2	AC-16, MP-2, MP-3, SC-16	1.4
ASM2.4.1	Asset Handling Procedures	T.1.3.3	A.7.2.2	AC-16, MP-2, MP-3, SC-16	17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8. 17.9
ASM2.4.2	Management of Removable Media	T.1.4.1	A.10.7.1	MP Family, PE-16	13.7, 13.8
ASM2.4.3	Removal and Movement of Information Assets	T.2.3.7	A.9.2.7	MP-5, PE-16	-
ASM2.5.1	Secure Information Asset or Media Disposal	T.1.4.2	A.10.7.2	MP-6	-
ASM2.5.2	Procedures for Re-Use of Assets	T.2.3.6	A.9.2.6	MP-6	16.7
ASM2.5.3	Records on Disposal	T.2.3.7	A.9.2.7	MP-5, PE-16	-
3. Physical and Environmental Security					
PHE3.1.1	Management Policy for Physical and Environmental Security	T2.1.1, T2.3.5	A.11.1.1	AC-19, AC-20, MP-5, PE-17	-
PHE3.2.1	Physical Security Perimeter	T2.2.1	A.11.1.1	PE-1	-

PHE3.2.2	Secure Areas Control Measures	T2.2.3	A.11.1.3	PE-3, PE-4, PE-5	-
PHE3.2.3	Secure Office & Meeting Rooms	T2.2.3	A.11.1.3	PE-3, PE-4, PE-5	-
PHE3.2.4	Protection against External & Environmental Threats	T2.2.4	A.11.1.4	CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15	-
PHE3.2.5	Effectiveness of Control Measures	T2.2.4	A.11.1.4	PE-1, PE-9, PE-10, PE-11, PE-13, PE-15, CP Family	-
PHE3.2.6	Working in Secure Areas	T2.2.5	A.11.1.5	AT-2, AT-3, PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8	-
PHE3.2.7	Physical Security Awareness	T2.2.5	A.11.1.5	AT-2, AT-3, PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8	17.3
PHE3.2.8	Delivery and Loading Areas	T2.2.6	A.11.1.6	PE-3 , PE-7, PE-16	-
PHE3.3.1	Equipment siting and protection	T2.3.1	A.11.2.1	PE-1, PE-18	1.6
PHE3.3.2	Supporting Utilities	T2.3.2	A.11.2.2	PE-1, PE-9, PE-11, PE-12, PE-14	-
PHE3.3.3	Cabling Security	T2.3.3	A.11.2.3	PE-4, PE-9	-
PHE3.3.4	Equipment Maintenance	T2.3.4	A.11.2.4	MA Family	1.6
PHE3.3.5	Removal of Equipment	T2.3.5	A.11.2.5	MP-5	1.6
PHE3.3.6	Security of Equipment Off-premises	T2.3.7	A.11.2.6	PE-17, PE-16	1.6
PHE3.3.7	Secure disposal or re-use of equipment	T.2.3.6	A.11.2.7	MP-6, SA-19(3)	-
PHE3.3.8	Unattended User Equipment	T.2.3.8	A.11.2.8	AC-11, IA-2, PE-3, PE-5, PE-18, SC-10	-
PHE3.3.9	Clear Desk & Clear Screen Policy	T.2.3.9	A.11.2.9	AC-11	-
4. Access Control Management					
ACM4.1.1	Access Control Policy	T5.1.1	A.9.1.1	AC-1	14.6
ACM4.2.1	User Registration and De-Registration	T5.2.1	A.9.2.1	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2	16.6
ACM4.2.2	Privilege Management	T5.2.2	A.9.2.3	AC-1, AC-2, AC-6, AC-21, PE-1, PE-2, SI-9	4.3
ACM4.2.3	Use and Management of Security Credential	T5.2.3	A.9.2.4	IA-5, IA-2	16.2, 16.4
ACM4.2.4	Use of secret authentication information	T5.3.1	A.9.3.1	IA-5	1.8
ACM4.2.5	Password management system	T5.5.3	A.9.4.3	IA-5	4.2, 4.4

ACM4.3.1	Access Control for Assets and Equipment in Teleworking Sites	T5.7.2	A.6.2.2	AC-1, AC-4, AC-17, AC-18, PE-17, PL-4, PS-6	-
ACM4.4.1	Review of User & Accounts Access Rights	T5.2.4	A.9.2.5	AC-2, PE-2	3.3
ACM4.5.1	Access to Network and Network Services	T5.4.1	A.9.1.2	AC-1, AC-5, AC-6, AC-17, AC-18, AC-20	1.7
ACM4.5.2	Remote User Authentication	T5.4.2	A.13.1.2	CA-3, SA-9	9.1
ACM4.5.3	Equipment Identification	T5.4.3	A.8.1.1	AC-19, IA-3	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.4, 15.1, 16.1
ACM4.5.4	Remote Diagnostic and Configuration Protection	T5.4.4	A.13.1.2	CA-3, SA-9	5.4
ACM4.5.5	Networks Connections Control	T5.4.5	A.9.1.2	AC-3, AC-6, AC-17, AC-18, SC-7	1.7
ACM4.5.6	Networks Routing Control	T5.4.6	A.9.1.2	AC-4, AC-17, AC-18	1.7
ACM4.5.7	Wireless Access Control	T5.4.7	A.9.1.2	AC-18	1.7
ACM4.6.1	Secure Log-On Procedures	T5.5.1	A.9.4.2	AC-7, AC-8, AC-9, IA-6	4.9, 12.11, 12.12
ACM4.6.2	User Identification and Authentication	T5.5.2	A.9.4.2	IA-2, IA-4, IA-5, IA-8	4.9, 12.11, 12.12
ACM4.6.3	Use of privileged utility programs	T5.5.4	A.9.4.4	AC-3, AC-6	4.1
ACM4.7.1	Information Access Restriction	T5.6.1	A.9.4.1	AC-3, AC-6, AC-14, CM-5	14.7
ACM4.7.2	Sensitive System Isolation	T5.6.1	A.9.4.1	AC-3, AC-6, AC-14, CM-5	2.1
ACM4.7.3	Publicly Accessible Content	T5.6.3	A.14.1.2	AC-22, SC-14	14.6
ACM4.8.1	Access Control to Program Source Code	T7.5.3	A.9.4.5	AC-3, AC-6, CM-5, CM-9, MA-5, SA-10	18.7
5. Operations Management					
OPM5.1.1	Operations Management Policies	T.3.2.2	A.12.1.1	SA-5	-
OPM5.2.1	Capacity Management	T3.3.1	A.12.1.3	AU-4, AU-5, CP-2, SA-2, SC-5	-
OPM5.2.2	System Acceptance and Testing	T3.3.2	A.14.2.9	SA-4, SA-12(7)	-
OPM5.3.1	Change Management	T3.2.3	A.12.1.2	CM-3, CM-5, CM-9, SA-10	11.3
OPM5.3.2	Separation of Test, Development and Operational Environment	T3.2.5	A.12.1.4	CM-4(1)*, CM-5*	18.9
OPM5.3.3	Software Configuration Restrictions and Baselining	T3.2.1	A.12.6.2	CM-5, CM-7(4), CM-7(5), CM-11	-
OPM5.3.4	Segregation of Duties	T3.2.4	A.6.1.2	AC-5	-

OPM5.4.1	Controls Against Malware	T3.4.1	A.12.2.1	AT-2, SI-3, SI-4(24)	7.7, 7.10, 8.1, 8.2, 8.4, 8.5, 8.6
OPM5.4.2	Perimeter Level Malware Protection	T3.4.1	A.12.2.1	AT-2, SI-3, SI-4(24)	7.7, 7.10, 8.1, 8.2, 8.4, 8.5, 8.6
OPM5.5.1	Backup Management	T3.5.1	A.12.3.1	CP-9	10.1, 10.3
OPM5.5.2	Archived Data Protection	T3.5.1	A.12.3.1	CP-10	10.1, 10.3
OPM5.6.1	Monitoring Procedures	T3.6.1	A.12.4.1	AU-3, AU-6, AU-11, AU-12, AU-14	6.2, 8.6, 8.7
OPM5.6.2	Audit Logging	T3.6.2, T3.6.5, T3.6.6	A.12.4.1	AU-3, AU-6, AU-11, AU-12, AU-14	6.2, 8.6, 8.7, 8.8
OPM5.6.3	Preservation of Log Information	T3.6.4	A.12.4.2	AU-9	6.4
OPM5.6.4	Administrators and Operators Logging	T3.6.3	A.12.4.3	AU-9, AU-12	4.8, 6.7, 14.9
OPM5.6.5	Clock Synchronization	T3.6.7	A.12.4.4	AU-8	6.1
OPM5.7.1	Technical Vulnerability Assessment	T7.7.1	A.12.6.1	RA-3, RA-5, SI-2, SI-5	3.7
OPM5.7.2	Preservation and Protection of Assessment Data	T7.7.1	A.12.6.1	RA-3, RA-5, SI-2, SI-5	3.7
OPM5.8.1	Information Systems Audit controls	M.5.5.1	A.12.7.1	AU-5*	8.8
6. Communications and Application Security Management					
CAM6.1.1	Communication Policy	T4.1.1	A.13.1.1	SC-1	1.7, 1.8, 7.4, 7.7, 7.9, 9.3, 9.4, 12.2, 12.3, 12.4, 12.6, 12.7, 12.8, 12.9, 13.3, 13.5, 14.2, 14.3, 14.4, 15.2, 15.3, 15.7, 15.8, 16.5
CAM6.2.1	Information Exchange Procedures	T4.2.1	A.13.2.1	AC-4, AC-20, AC-21, CA-3, PA-4, SC-7, SC-8	-
CAM6.2.2	Security of Information Transfer	T4.2.1	A.13.2.1	AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9	-
CAM6.2.3	Agreements on Information Transfer	T4.2.2	A.13.2.2	CA-3, SA-9	-
CAM6.2.4	Security Awareness for Partners and Third Parties	T4.2.2	A.13.2.2	CA-3, SA-9	-
CAM6.2.5	Physical Media in Transit	T4.2.3	A.13.2.1	MP-5	-
CAM6.2.6	Electronic Messaging	T4.2.4	A.13.2.3	SC-8	7.8, 13.4
CAM6.2.7	Business Information System Security	T4.2.5	A.14.1.2	CA-1, CA-3	-

CAM6.3.1	Security of Electronic Commerce Services	T4.3.1	A.14.1.2	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14	18.10,
CAM6.3.2	Security of Public Services and Information	T4.3.3	A.14.1.2	SC-14	9.5, 18.10
CAM6.3.3	Digital Transactions	T4.3.2	A.14.1.3	SC-3, SC-7, SC-8, SC-9, SC-14	9.5, 18.10
CAM6.4.1	Network Controls	T4.5.1	A.13.1.1	AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23	1.7, 1.8, 7.4, 7.7, 7.9, 9.3, 9.4, 12.2, 12.3, 12.4, 12.6, 12.7, 12.8, 12.9, 13.3, 13.5, 14.2, 14.3, 14.4, 15.2, 15.3, 15.7, 15.8, 16.5
CAM6.4.2	Security of Network Services	T4.5.2	A.13.1.2	SA-9, SC-8, SC-9	9.1
CAM6.4.3	Networks Segregation	T4.5.3	A.13.1.3	AC-4, SA-8, SC-7	9.2, 11.7, 14.1, 15.10
CAM6.4.4	Wireless Networks	T4.5.4	A.13.1.2	AC-4, SA-8, SC-7	9.1
CAM6.5.1	Information Security Requirements Analysis and Specification	T7.2.1	A.14.1.1	SA-1, SA-3, SA-4	-
CAM6.6.1	Input Data Validation	T7.3.1	A.14.2.5	SI-9, SI-10	5.1
CAM6.6.2	Output Data Validation	T7.3.4	A.14.2.5	SI-15	5.1
CAM6.6.3	Internal Processing Capabilities	T7.3.2	A.14.2.8	SI-7, SI-9, SI-10	-
CAM6.6.4	Message Integrity	T7.3.3	A.14.2.5	AU-10, SC-8, SI-7	5.1
CAM6.6.5	Fault Tolerance and Continuity	T7.3.2	A.14.2.5	SI-7, SI-9, SI-10	5.1
CAM6.7.1	Management Policy for Cryptographic Controls	T7.4.1	A.10.1.1	SC-12	13.9, 14.4, 14.8, 15.7, 16.4, 16.5, 18.5
CAM6.7.2	Cryptographic Key Management	T7.4.2	A.10.1.2	SC-17	13.5, 13.6
CAM6.8.1	Software Installation on Live Systems	T7.5.1	A.12.5.1	CM-3, CM-5, CM-7(4), CM-7(5), CM-11	2.6
CAM6.8.2	Protection of System Test Data	T7.5.2	A.14.3.1	SA-3(2)*, AC-3, AC-4	-
CAM6.9.1	Outsourced Software Development	T7.6.5	A.14.2.7	SA-1, SA-4, SA-6, SA-7, SA-8, SA-9, SA-11, SA-12, SA-13	18.1,
CAM6.10.1	Non-Disclosure and Confidentiality	M.1.3.2	A.13.2.4	PS-6	-
7. Healthcare Information Security					
HIS7.1.1	Health Information Protection Policy	M5.2.4	A.5.1.1	PL-5; SI-12	-

HIS7.2.1	Security of Healthcare Information	M5.2.4	A.18.1.4	PL-5; SI-12	-
HIS7.3.1	Medical Devices Management Procedures	T3.2.2	A.12.1.1	AC-19, IA-3	-
HIS7.3.2	Access Allocation for Medical Devices	T5.4.1	A.9.1.2	AC-6	1.7
HIS7.3.3	Security of Information within Medical Devices	T7.3.2	A.14.2.8	N/A	2.5
HIS7.3.4	Communication Facility for Medical Devices	T5.7.1	A.6.2.1	N/A	13.6
HIS7.4.1	Access Control for Portable and Medical Devices	T5.7.1	A.6.2.1	AC-1, AC-17, AC-18, AC-19, PL-4, PS-6	13.6
8. Third Parties and Supply Chain Management					
TSM8.1.1	Security Policy for Supply Chain and Third-Parties Management	T6.1.1	A.15.1.1	PS-7	-
TSM8.2.1	Secure Third-Party Service Agreements	T6.2.1	A.15.1.2	SA-9	-
TSM8.2.2	Monitoring and Review of Third-Party Services	T6.2.2	A.15.2.1	SA-9	-
TSM8.2.3	Managing Changes to Third Party Services	T6.2.3	A.15.2.2	RA-3, SA-9	-
TSM8.3.1	Information Systems Acquisition, Development and Maintenance Policy	T7.1.1, T7.4.1	A.10.1.1, A.14.2.1	SA-1, MA-1, SI-1 IA-7, SC-8, SC-9, SC-12, SC-13	13.9, 14.4, 14.8, 15.7, 16.4, 16.5, 18.1, 18.5
TSM8.4.1	Supplier Reviews	T7.8.2	A.15.2.1	SA-12	-
TSM8.4.2	Secure Supply Chain Operations	T7.8.4	A.15.2.2	SA-12	-
TSM8.4.3	Reliable Delivery of Items and Services	T7.8.4	A.15.2.2	SA-12	-
TSM8.4.4	Contingency Planning of Critical Supplies	T7.8.6	A.15.2.1	SA-14	-
9. Security Incident Management					
SIM9.1.1	Information Security Incident Management Policy	T8.1.1	A.16.1.1	IR-1	19.1
SIM9.2.1	Incident Response Procedures	T8.2.1	A.16.1.1	IR-8	19.1
SIM9.2.2	Incident Response Team Responsibilities	T8.2.2	A.16.1.1	IR-10	19.1
SIM9.2.3	Security Incident Assessment and Classification	T8.2.3	A.16.1.4	AU-6, IR-4	19.8
SIM9.2.4	Response to Information Security Incidents	T8.2.5	A.16.1.5	IR-3	-
SIM9.2.5	Incident Evidence Collection	T8.2.7, T8.2.9	A.16.1.7	AU-9, IR-4	-
SIM9.2.6	Learning from Incidents	T8.2.4, T8.2.8	A.16.1.6	IR-2, IR-4	-
SIM9.3.1	Reporting Information Security Events	T8.3.2	A.16.1.2	AU-6, IR-1, IR-6, SI-4, SI-5	19.5
SIM9.3.2	Reporting Security Weakness	T8.3.3	A.16.1.3	PL-4, SI-2, SI-4, SI-5	19.4
10. Information Systems Continuity Management					
SCM10.1.1	Information Systems Continuity Management Policy	T9.1.1	A.17.1.1	CP-1	-

SCM10.2.1	Developing Information System and Application Continuity Plans	T9.2.1	A.17.1.2	CP-2	-
SCM10.2.2	Implementing Information System and Application Continuity Plans	T9.2.2	A.17.1.3	CP-2	10.2
SCM10.2.3	Testing, Maintaining and Reassessing Plans	T9.3.1	A.17.2.1	CP-4, CP-5	-