



NATIONAL CYBER SECURITY ACCREDITATION PROGRAM

DISCLAIMER

This document is the sole property of UAE Cyber Security Council and is approved by the UAE Cabinet.

The UAE Cyber Security Council reserves the right to amend, add, or delete any section of this Policy.

Neither the whole nor part of this document shall be reproduced without the prior written consent of the UAE Cyber Security Council.



VERSION CONTROL

Version 0.1

Date: 11 May 2022
Prepared by: CSC
Amendment Content: Initial Draft Document

Version 0.2

Date: 25 June 2022
Prepared by: CSC
Amendment Content: Updated based on initial feedback

Version 1.0

Date: 30 August 2022
Prepared by: CSC
Amendment Content: Updates as per review comments on the draft v0.2 of the document

Reviewed by

Approved by


Designation:	XXXXXXXXX	XXXXXXXXX
Name:	XXXXXXXXX	XXXXXXXXX
Signature:	XXXXXXXXX	XXXXXXXXX
Date:	XXXXXXXXX	XXXXXXXXX

Table of Contents

1. Introduction	05
1.1 Purpose	07
1.2 National Lead Agency	08
1.3 Scope and Applicability	09
1.4 Guiding Principles	11
1.5 Strategic Objective	14
2. National Cybersecurity Accreditation Governance Model	15
3. Implementation	21
4. Monitoring and Performance Management	23
5. Gaining Accreditation	25
5.1 Overview	26
5.2 Process	27
5.3 Mandatory Accreditation Track Process Flowchart	29
5.4 Voluntary Accreditation Track Process Flowchart	30
5.5 Maturity Modelling	31
5.6 Cross Recognition of Existing Accreditation	32
6. Auditing and Maintaining Compliance	34
6.1 Audit Process	35
6.2 Maintaining Compliance	36

Table of Contents

7. Application of the National Cybersecurity Accreditation Controls Framework	37
7.1 Governance	38
7.2 Applicability of Controls	39
8. Appendices	40
8.1 Annex A: Reference Documents - UAE Policies and Standards	41
8.2 Annex B: Outline of an Independent Assessors Program	42
8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List	45
8.4 Annex D: Abbreviations	68

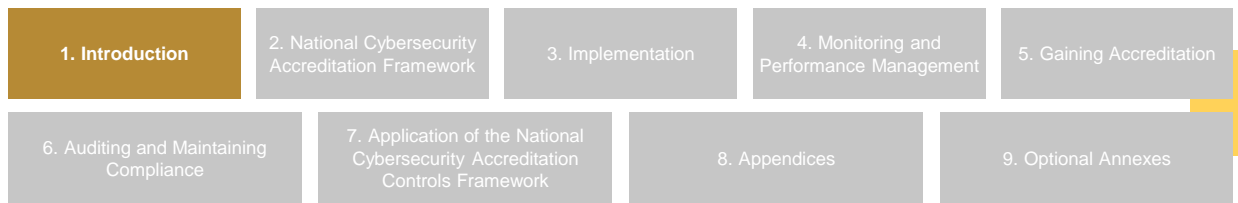


SECTION 1
INTRODUCTION

INTRODUCTION

The UAE is committed to the further development of its digital infrastructure, as well as its cyberspace, to support economic development and provide an environment where the interests of its government, businesses, and citizens can thrive. The National Cyber security Accreditation Program (NCAP) is an initiative that aims to cultivate trust in the UAE cyber ecosystem through raising its security maturity in a transparent way. Based on international best practice, the program balances security and efficiency in this national level assurance effort.

The NCAP will enable UAE government and Entities the ability to demonstrate their conforming to baseline cyber security requirements, and grant the ability to work with provider entities who also conform to baseline cyber security requirements. This national level baseline will provide assurance to stakeholders that these entities adhere to best practices and will continue to maintain a minimum standard of cyber security maturity. This will ensure a consistent level of cyber security services are provided across the country, driving up standards and quality of service across the UAE.

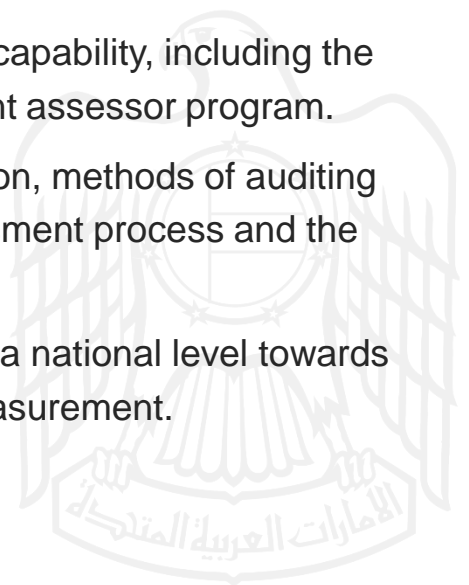


1.1 Purpose

The NCAP is intended as a two-track cyber security accreditation program, and utilizes well known and documented security controls from the UAE Information Assurance Regulation throughout the accreditation process. Government organizations, Entities that are identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy, and entities providing services to Government, specifically Cyber security Service Providers, Cyber security Training Providers, and Cyber security Audit Providers will be required to attain certification on a mandatory basis, while other entities may choose to join the program to raise the maturity of their cyber security program and gain a trusted certification.

The framework aims to build confidence among consumers and stakeholders (owners, partners, citizens, etc.) for accredited entities and raise national cyber maturity across the UAE. An Independent Assessors Program (IAP) will be launched to play a force-multiplication role in rolling out and maintaining the NCAP Program throughout the UAE. This document outlines various components of the NCAP, including implementation and maintenance, giving a high-level overview of the following:

- The program elements including the national capability, including the framework model, and the related independent assessor program.
- The dual-track process for gaining accreditation, methods of auditing and maintaining accreditation, the self-assessment process and the supporting controls framework.
- The monitoring and evaluation mechanism at a national level towards continued conformance and performance measurement.



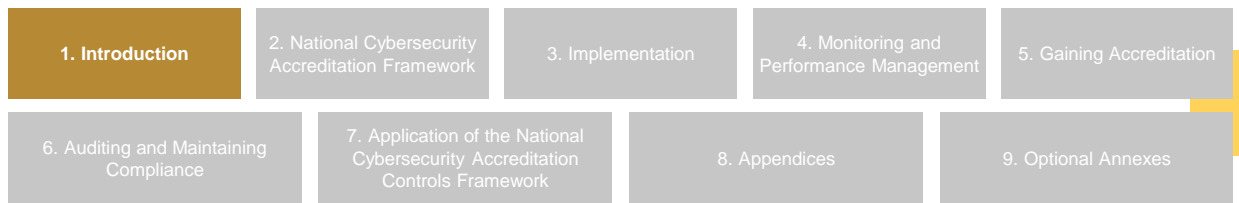
1. Introduction	2. National cyber security Accreditation Framework	3. Implementation	4. Monitoring and Performance Management	5. Gaining Accreditation
6. Auditing and Maintaining Compliance	7. Application of the National cyber security Accreditation Controls Framework	8. Appendices	9. Optional Annexes	



1.2 National Lead Agency

The National Lead Agency will be designated for establishment, maintenance and implementation of the NCAP. The National Lead Agency, has an overall implementer role and serves as a central ‘point-of-contact’ on a national level across the UAE for the NCAP.

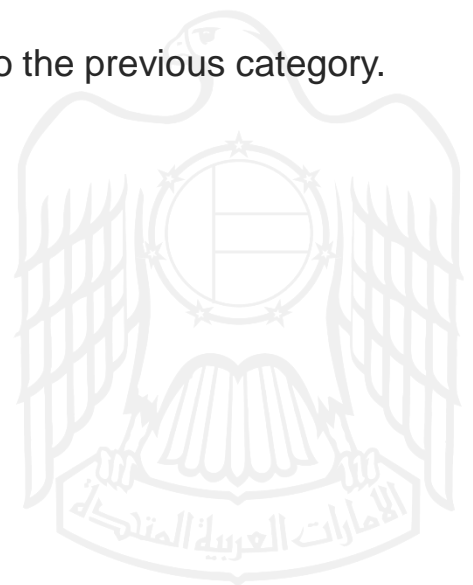


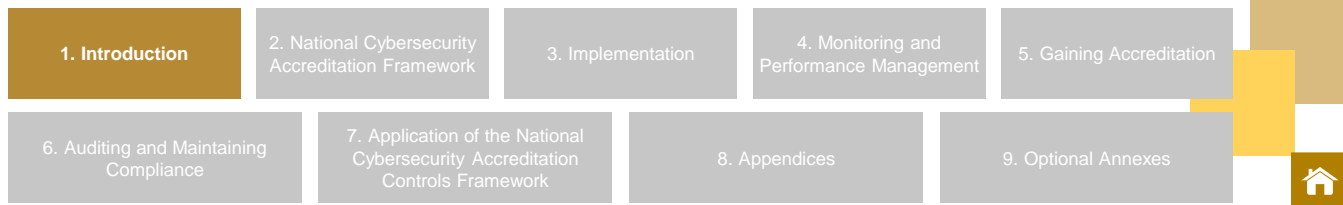


1.3 Scope and Applicability

The NCAP is broadly applicable to all Government and private sector Entities of the UAE, Entities offering services to the UAE, and UAE Government and private sector Entities operating abroad (through independent assessor program), on either a mandatory or voluntary basis:

- **Government Entities:** Organizations that are part of the UAE Government, whether departments or businesses owned or operated by Government Entities.
- **Critical Infrastructure:** Entities that are identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy.
- **Cyber security Service Providers:** Refers to all organizations in the UAE providing services that aim to mitigate cyber risks; protect, detect, respond and recover against cyberattacks, including providers of technology, managed services and process consultants.
- **Cyber security Training Providers:** refers to organizations providing professional certifications to individuals in the UAE.
- **Cyber security Audit Providers:** refers to organizations that provide auditing services to entities within the UAE.
- **Other Entities:** Any entity that does not fall into the previous category.





Following a risk-based approach to balance security requirements and efficiency, the NCAP has a mandatory and a voluntary (self-assessment) accreditation paths that constitute a dual-track accreditation program. This policy applicability is as follows:

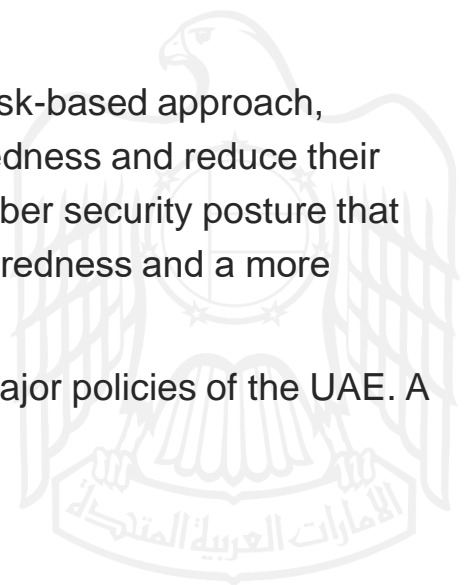
Mandatory track: All Government Entities, and entities providing services to UAE government sector, those sectors that are identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy, and Entities providing services to Government (Specifically Cyber security Service Providers, Cyber security Training Providers and Cyber security Audit Providers) are required to follow the mandatory certification requirements of the NCAP.

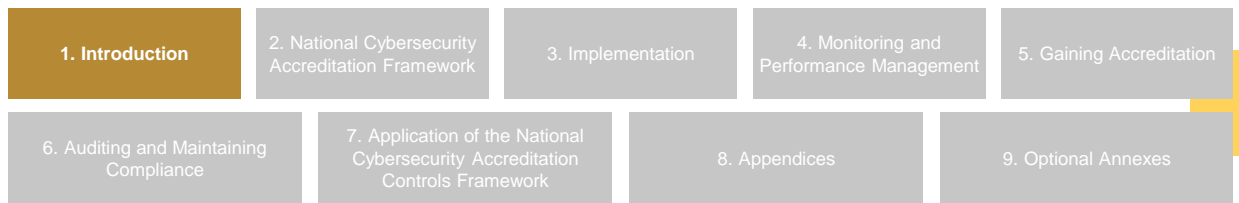
Voluntary track: Any entity in the UAE may participate in the program through self-assessment. These entities can decide to participate in the program to fulfil UAE regulatory requirements (above) or to obtain official proof of their cyber security maturity accepted throughout the UAE.

The primary focus of the program is to provide an appropriate level of assurance based on information value and organizational risk appetite, and is specifically targeted toward Government entities, and entities engaging with the UAE government and identified critical information infrastructure sectors.

Through a certification process, and following a risk-based approach, stakeholders improve their cyber security preparedness and reduce their risk profile, leading to a more secure individual cyber security posture that ultimately contributes to the UAE's national preparedness and a more secure cyberspace environment.

The NCAP shall be aligned with other relevant, major policies of the UAE. A list of those policies is provided in Annex A.





1.4 Guiding Principles

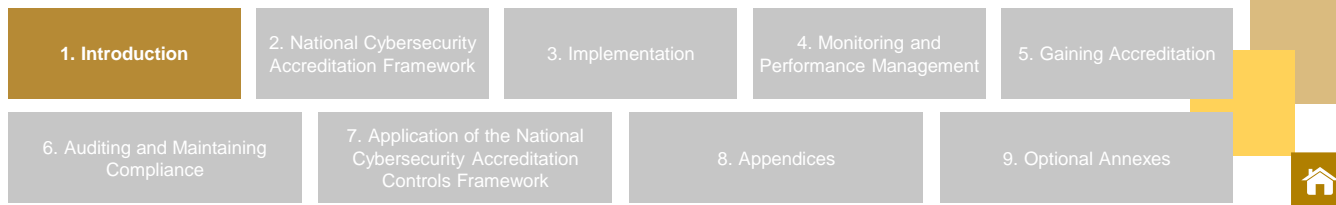
The NCAP is predicated on internationally acknowledged guiding principles – high-level governing approaches –which are outlined to establish a common understanding amongst stakeholders in the UAE cyberspace. Each guiding principle below is then mapped to the corresponding control set from the UAE Information Assurance Regulation. The principles are listed below:

- Govern: Identify and manage security risks.
- Protect: Implement security controls to reduce security risks.
- Detect: Detect and understand cyber security events to identify cyber security incidents.
- Respond: Respond to and recover from cyber security incidents.

Govern principles

- UUAE-IA-M2: Information Security Risk Management
- UAE-IA-M5: Compliance
- UAE-IA-T1: Asset Management
- AE-IA-M1: Strategy and Planning





Protect principles

- UAE-IA-M3: Awareness and Training.
- UAE-IA-M4: Human Resources Security
- UAE-IA-M6: Performance Evaluation and Improvement
- UAE-IA-T2: Physical and Environmental Security
- UAE-IA-T3: Operations Management
- UAE-IA-T4: Communications
- UAE-IA-T5: Access Control
- UAE-IA-T6: Third-Party Security
- UAE-IA-T7: Information System Acquisition, Development and Maintenance

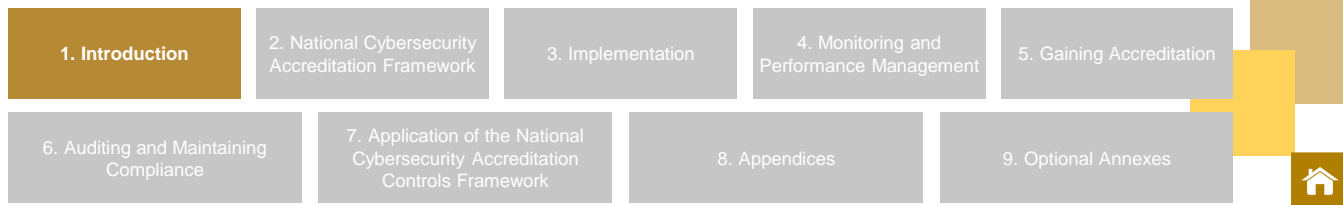
Detect principles

- UAE-IA-T3.6: Monitoring

Respond principles

- UAE-IA-T8: Information Security Incident Management
- UAE-IA-T9: Information System Continuity Management





Maturity modelling

When implementing the cyber security principles using the UAE Information Assurance Regulation controls, an entity will be assessed against the following maturity model to assess the implementation of individual principles, groups of principles, and the cyber security principles. The four levels in the maturity model are:

Level I: Initial

Minimal or ad-hoc compliance with guiding principles.

Level II: Developing

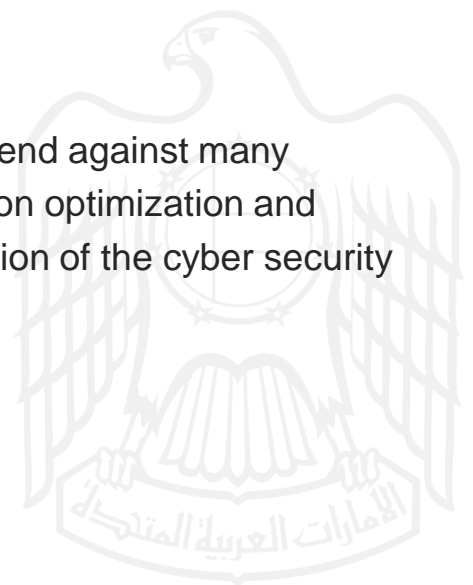
Basic compliance requirements are met, controls are in place to defend against common, non-targeted attackers.

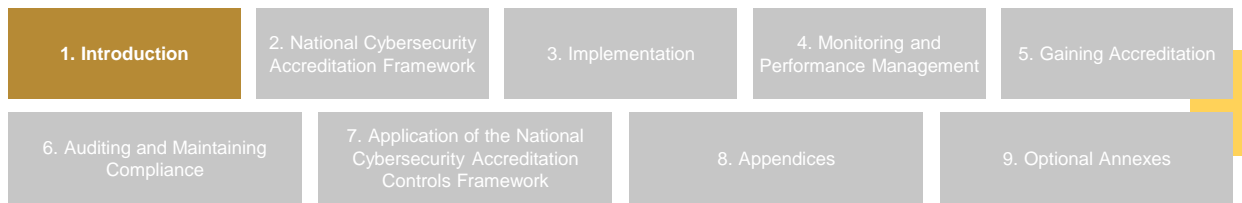
Level III: Managing

Intermediate level of compliance requirements met - Controls in place to defend against common targeted attackers. The cyber security principles are established as standard business practices and robustly implemented throughout the organization.

Level IV Optimizing

High level of compliance. Controls in place to defend against many Advanced Persistent Threats. A deliberate focus on optimization and continual improvement exists for the implementation of the cyber security principles throughout the organization.

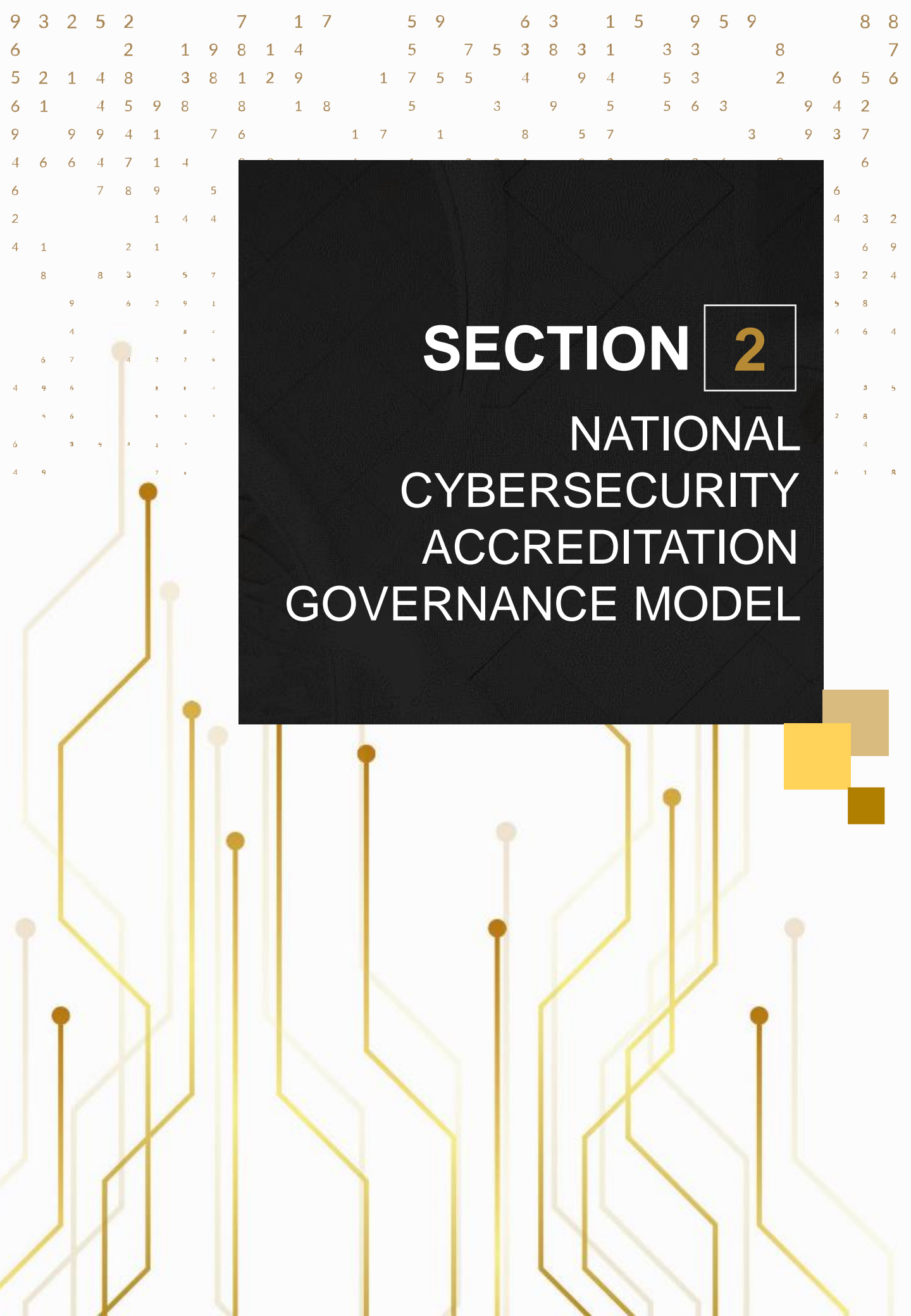




1.5 Strategic Objectives

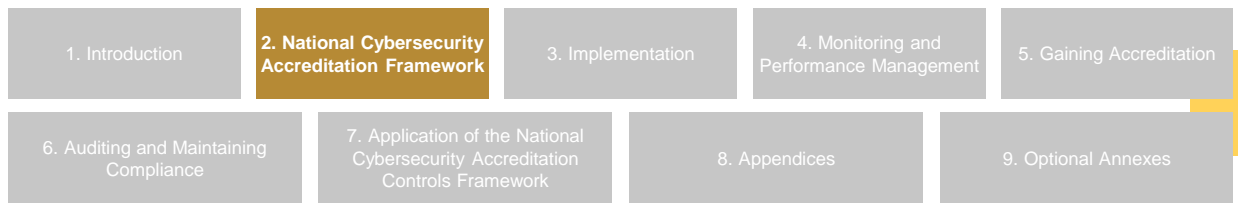
The following objectives aim to provide a significant uplift to the UAE Cyber Security environment:

<p>Create a UAE Specific Framework</p>	<p>Build a UAE specific framework that leverages existing and well known, functional global accreditation frameworks to build and enhance the UAE’s reputation as a global center of excellence for cyber security services.</p>
<p>Promote the Adoption of Standardized National Cyber Security Controls</p>	<p>The NCAP utilizes standardized security controls, as presented in the UAE Information Assurance Regulation. This ensures consistent application of controls across the UAE and reduces the potential for confusion or competing standards.</p>
<p>Empower Entities to Prioritize Cyber Security using a Risk based approach</p>	<p>The framework uses an intelligent, risk-based approach to prioritize cyber security services that are most important to the UAE’s national security and provide recognition of accredited entities to enhance the growth of the cyber security system in the UAE.</p> <p>At a basic level, a risk-based approach seeks to match risk levels with appropriate mitigation strategies to provide, balanced, cost-effective approach to cyber security that balances business needs with cyber security.</p>
<p>Promote Shared Responsibility (‘Unity of Effort’)</p>	<p>Stakeholders of the UAE at the national, emirate and entity levels need to work together on a ‘Unity of Effort’ basis to be effective in maintaining the stability of UAE cyberspace and invest in reasonable efforts to raise its cyber security maturity. Entities (esp. critical infrastructure operators) and national level stakeholders (government ministries, agencies) are collectively responsible to take effective steps to contribute to the achievement of this goal. The NCAP serves as an overarching framework for this national effort to deliver on these ambitions in a collaborative, efficient way in a complex, multi-stakeholder environment.</p>



SECTION **2**

NATIONAL CYBERSECURITY ACCREDITATION GOVERNANCE MODEL



2.1.1 Mandatory Accreditation Track

UAE Government entities, Entities that are identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy , and Entities providing services to Government (Specifically Cyber security Service Providers, Cyber security Training Providers and Cyber security Audit Providers) are required on a mandatory basis to participate in the program and acquire and maintain the relevant level of NCAP certification. Participation in the NCAP can also be mandated by law, regulation, or requirement by relevant UAE government entities. This is especially relevant in public-private cooperation schemes or procurement programs where a risk-based approach makes mandating accreditation under the NCAP program practical.

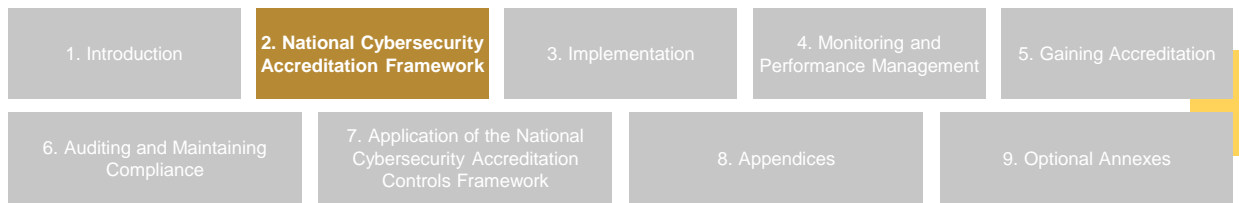
National Cyber security Accreditation Program Certificates can only be issued by the National Lead Agency after receiving formal proof of the successful closure of the attestation process. The National Lead Agency maintains a database about certificates issued (including validity) and will provide a method to confirm accreditation for concerned entities.

The attestation process is designed to be carried out by the National Lead Agency utilizing an Independent Assessor Program (IAP) as a flexible and resource-efficient approach to extend its services. The IAP Program allows for the inclusion of vetted, professional organizations and individuals with the necessary skills and resources to attest conformity with NCAP requirements. This allows the National Lead Agency to leverage private sector resources for the successful implementation of the NCAP following a force-multiplier model. An outline of the independent assessor program is provided in Annex B.

Entity maturity will be measured against the NCAP Maturity Model, outlined in Section 5.

The overarching goal of the Mandatory Track is to provide assurance to and require conformity from identified entities within the UAE with relevant cyber security controls based on the UAE Information Assurance Regulation. The mandatory track is applicable to UAE government organizations, those Entities that are identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy, and entities providing services to Government (specifically Cyber security Service Providers, Cyber security Training Providers, and Cyber security Audit Providers).





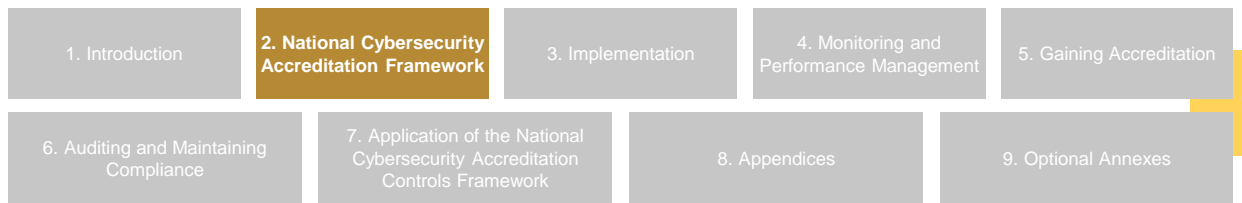
2.1.1 Mandatory Track

2.1.1.1 Cybersecurity Service Providers

Entities providing cyber security services to Government agencies must maintain compliance with the requirements of the NCAP.

Additionally, Cyber security Service Providers must be able to demonstrate competence in the area for which their cyber security services have been engaged. For example, an entity seeking to provide penetration testing services to Government must be able to demonstrate compliance with NCAP requirements, and that personnel have an appropriate level of competence through maintaining industry recognized certifications Likewise, an entity seeking to provide incident response services to Government must be able to demonstrate competence through maintaining certifications





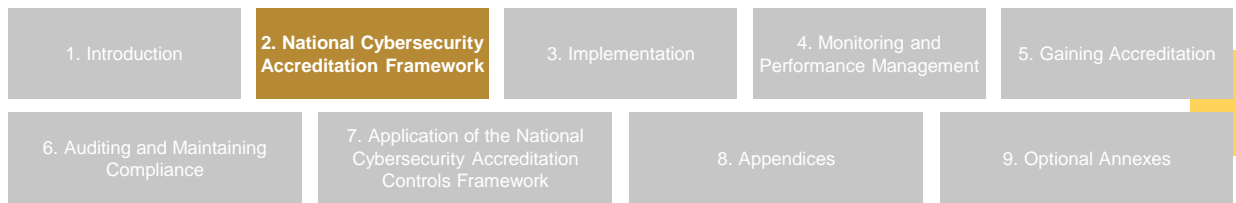
2.1.1 Mandatory Track

2.1.1.2 Cybersecurity Training Providers

Entities providing training services to Government agencies must maintain compliance with the requirements of the NCAP.

Additionally, cyber security training providers must be able to demonstrate competence in the area in which they are providing training services, must be a recognized training provider of the training originating body, and be able to demonstrate that personnel have an appropriate level of competence relevant to the training being provided. Personnel can demonstrate competence by maintaining certifications required by the training originating body.





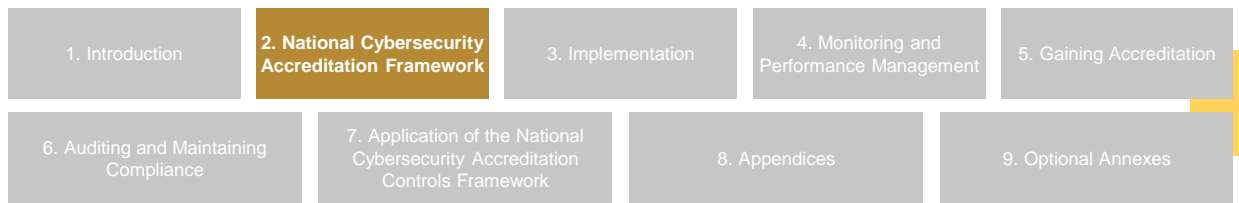
2.1.1 Mandatory Track

2.1.1.3 Cybersecurity Audit Providers

Entities providing cyber security auditing services to Government agencies must maintain compliance with the requirements of the NCAP.

Additionally, Cyber security Audit Providers must be able to demonstrate competence in the area in which they are providing audit services, must demonstrate compliance with NCAP baseline requirements and must demonstrate that personnel have an appropriate level of competence through maintaining industry recognized qualifications.





2.1.2 Voluntary Accreditation Track (Self-assessment)

The voluntary accreditation track of the NCAP enables Entities to participate in the NCAP certification program through self-assessment. The voluntary track is available for all Entities that are not identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy or required to attain accreditation for Government engagement. These Entities can decide to participate in the program to fulfil UAE regulatory requirements as a gateway to providing services to Government, or to self-attest as provide proof of their cyber security maturity through a trusted certification that they can leverage with their own stakeholders (owners, partners, clients, etc.).

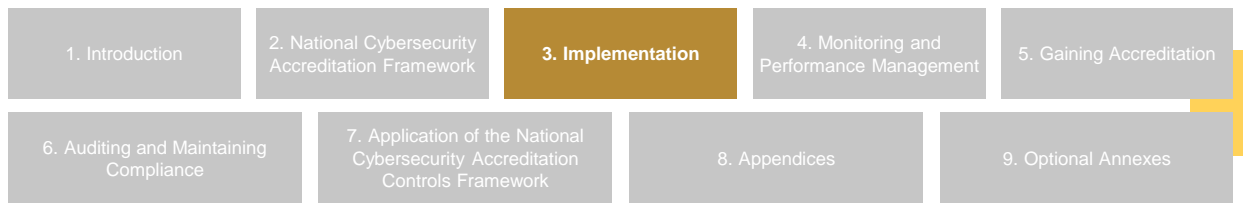
Certification gained via self-assessment and is signed by the CEO (or equivalent) of the private sector entity ensuring the integrity and credibility of the attestation process, and must be registered with the National Lead Agency. Entities that successfully complete the self-certification process become eligible for the NCAP Voluntary Certificate and machine generated NCAP Self-certification Report issued by the UAE Cyber Security Council.

Additionally, entities that self-certify will be audited on a random basis by the National Lead Agency to ensure the integrity of the process.



The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, elongated ovals. The overall color palette is a mix of light beige, olive green, and dark brown. On the right side, there are vertical lines resembling a circuit board or data stream, with small circles at various intervals. In the center, a large black rectangle contains the section title in white and gold text.


SECTION 3
IMPLEMENTATION



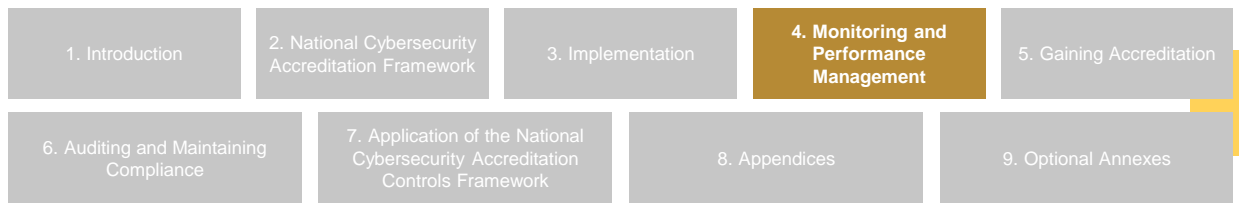
Implementation and operationalization of the NCAP will be led by the UAE Cyber Security Council as the National Lead Agency including developing and implementing processes and procedures to evolve the capabilities and maturity of the program (including roll-out of the Independent Assessor Program).

Supporting procedures and enabling capabilities, tools, and systems will be developed, maintained, and updated by the National Lead Agency.

Accordingly, UAE Cyber Security Council will work with relevant national stakeholders to implement the UAE NCAP, to establish a fully operational national capability, then continue to raise its maturity through systemic revision cycles.

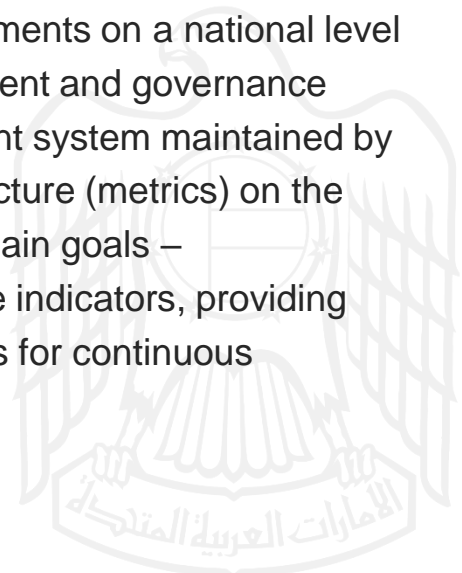
The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, irregular shapes. The overall color palette is a mix of light beige, olive green, and dark brown. On the right side, there are vertical lines resembling a circuit board or data stream. A large, solid black rectangle is positioned in the lower-middle section, containing the text.

SECTION 4
**MONITORING AND
PERFORMANCE
MANAGEMENT**



A detailed system to monitor the implementation of the NCAP shall be rolled out as part of the program implementation. Deployed by the National Lead Agency, this function is necessary to make the NCAP measurable. Being able to measure the accreditation program and its results, in turn, is essential to create visibility and serves as the foundation for continuous improvement. Such a monitoring function shall have multiple components, including those providing visibility and key metrics for assessed entities, statistics about typical deficiencies or gaps identified and other, similar metrics (collected on a statistical, anonymized basis) describing the maturity of a sector or the UAE cyber ecosystem on a national, aggregate level. Such statistical information is invaluable in providing general situational awareness and understanding of the strategic picture of the UAE cyber security posture and maturity, key risks and potential mitigation strategies.

Performance management is a related, subsequent function of the NCAP that is essentially leveraging data provided by the above monitoring function and compares that input to pre-set Key Performance Indicators (KPI) to provide an objective basis for evaluating the actual performance of the NCAP. Relevant KPIs can be defined based on international benchmarks provided by specialist professional sources. Ideally, such metrics can be connected to relevant risk assessments on a national level and serve as a key input informing risk management and governance activities. Ultimately the performance management system maintained by the National Lead Agency shall provide a clear picture (metrics) on the efficiency of the NCAP Program considering its main goals – operationalized through relevant key performance indicators, providing clear visibility on implementation and a solid basis for continuous improvement.

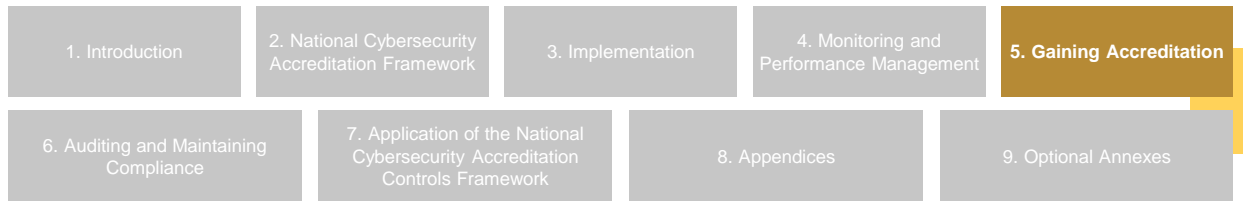




SECTION **5**

GAINING ACCREDITATION



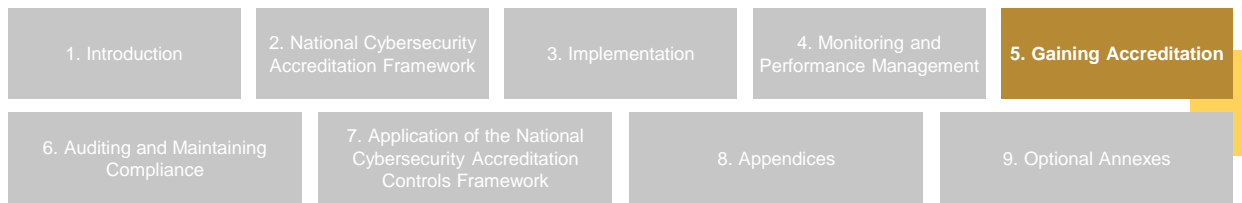


5.1 Overview

UAE government and Entities can get certification under the NCAP through a dual-track system. Identified entities are mandated to participate and their assessment is carried out by the National Lead Agency either directly, through an Authorized Government Entity, or through the Independent Assessors Program. Formal certification is issued by the National Lead Agency. Additional information about Authorized Government Entities and Authorized Independent Assessors is available in Annex B.

All other UAE entities may decide to gain accreditation following a voluntary self-assessment process that they can leverage to understand their cyber security maturity, identify gaps in their control environment and to provide proof to their stakeholders about their cyber security credentials. This process may also be aided by outside assessors participating in the Independent Assessors Program.





5.2 Process

5.2.1 Mandatory Accreditation Track

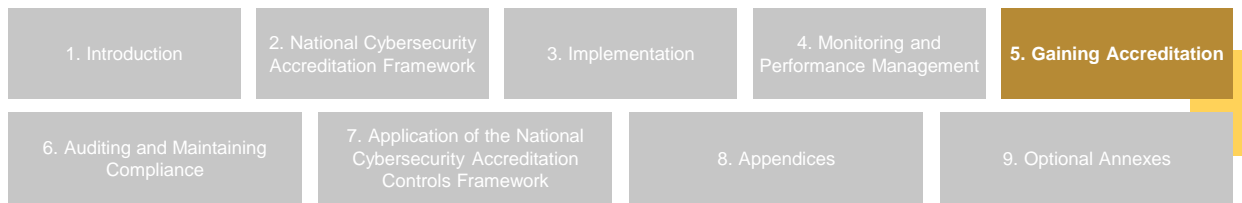
Mandated organizations, including UAE government organizations and those Entities that are identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy, and entities providing services to Government, specifically Cyber security Service Providers, Cyber security Training Providers, and Cyber security Audit Providers are required on a mandatory basis to participate in the program and acquire and maintain NCAP certification.

Mandated organizations are required to initiate their certification process themselves by reaching out to the National Lead Agency. In turn, the National Lead Agency is to carry out the assessment following detailed procedures defined in a Standard Operating Procedure either directly, through an Authorized Government Entity, or through the Independent Assessor Program.

The attestation process aims to assess evidence provided by the entity against the National Cyber security Accreditation Controls Framework made available as part of the NCAP Program. The assessment must be carried out in a documented way defined by the NCAP Assessment Standard Operating Procedure. Controls irrelevant in the context of the networks, systems and assets of the entity under assessment can be scoped out providing documented rationale in line with the requirements of the NCAP Assessment Standard Operating Procedure.

The attestation process must be completed within 6 months after its initiation by the entity. In case substantive control deficiencies are identified, the entity can be provided with a 3 or 6 months window to remediate deficiencies and provide proof of conformity with the given controls. In case the entity is unable to fulfil this requirement then the certification process shall be closed without issuance of a certificate.

Upon successful closure of the attestation process and if the entity has provided all required proof of conformity with the National Cyber security Accreditation Controls Framework an NCAP Certificate is to be issued by the National Lead Agency.



5.2 Process

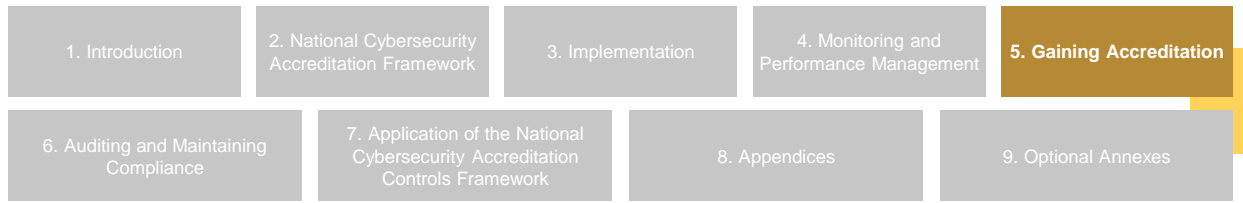
5.2.2 Voluntary Accreditation Track (Self-assessment)

The second track of the NCAP serves as a voluntary, self-assessment based assurance program available for any Entities in the UAE. This group of stakeholders includes all Entities that are not identified under the UAE Critical Information Infrastructure Protection (CIIP) Policy, or required to attain accreditation for Government engagement (as is the case for Cyber security Service Providers, Cyber security Training Providers and Cyber security Audit Providers engaged to provide services to Government entities), but still wish to assess their cyber security maturity, remediate gaps and demonstrate to their stakeholders their effort to be a trusted member of the UAE cyberspace ecosystem.

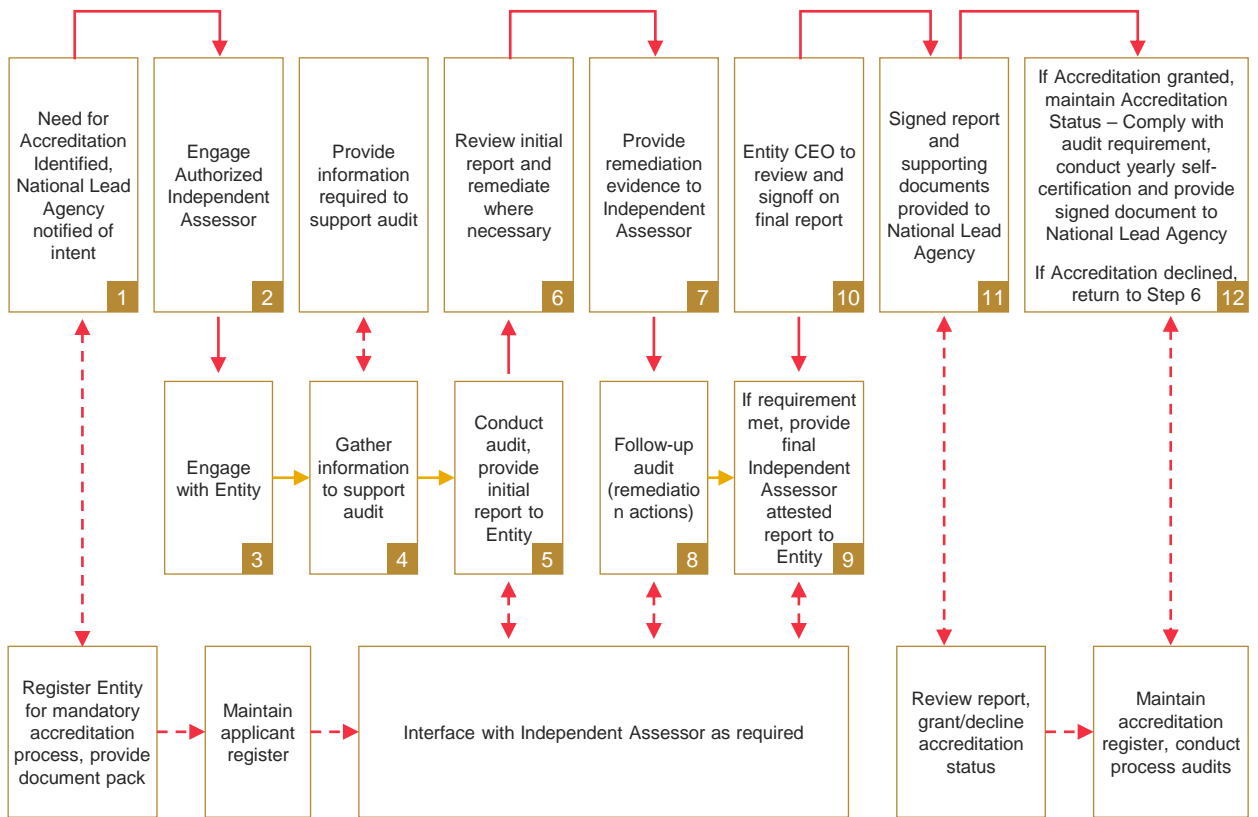
Formal completion of the self-certification process requires the CEO (or equivalent) of the private sector entity to sign the NCAP Self-certification documentation ensuring the integrity and credibility of the attestation process.

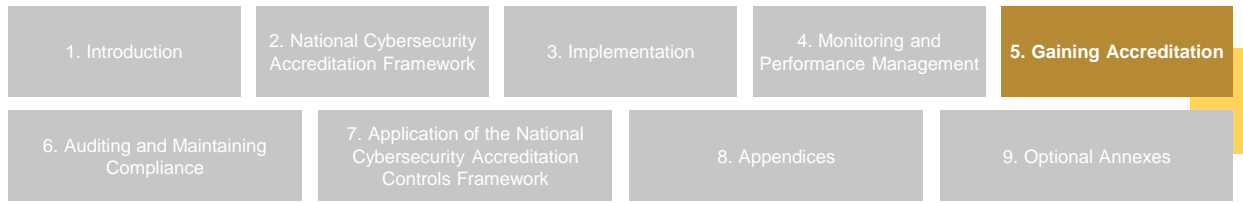
Participants successfully completing the requirements of the self-certification process become eligible for the NCAP Voluntary Certificate, the machine generated NCAP Self-certification Report issued by the UAE Cyber Security Council. Participating entities then can demonstrate that they fulfil the requirements of the NCAP through exhibiting electronic emblem of the NCAP Program on their public facing websites and print publications in line with standards defined by the UAE Cyber Security Council.

The streamlined self-certification track of the NCAP enables organizations within the UAE cyber ecosystem to assess and enhance their cyber security posture in a cost-effective way and inform their stakeholders and the broader UAE national cyber community about their commitment and efforts.

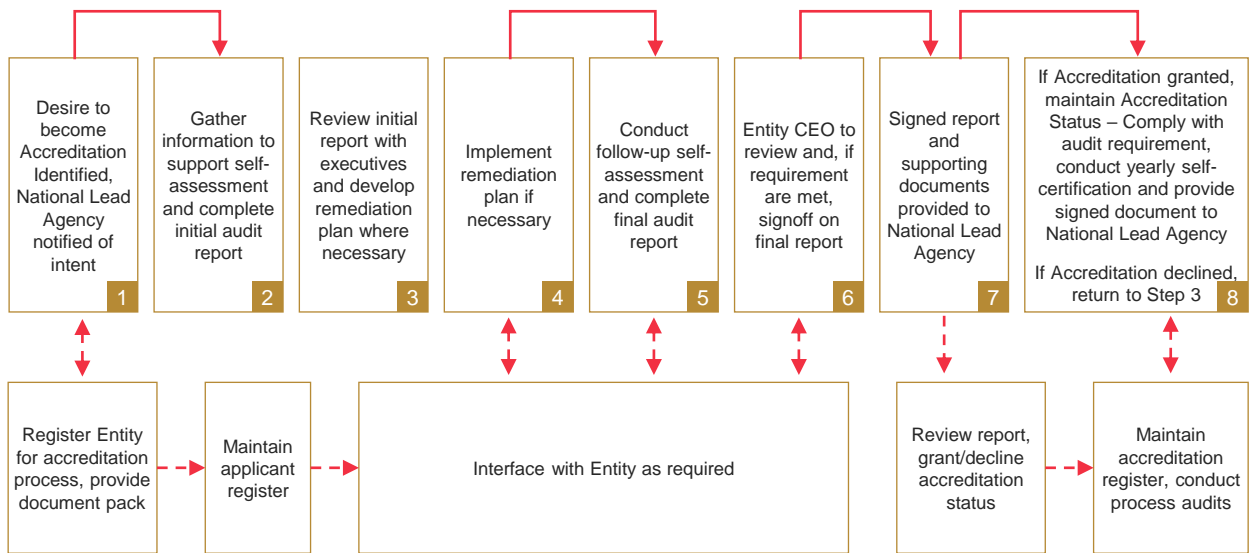


5.3 Mandatory Accreditation Track Process Flowchart



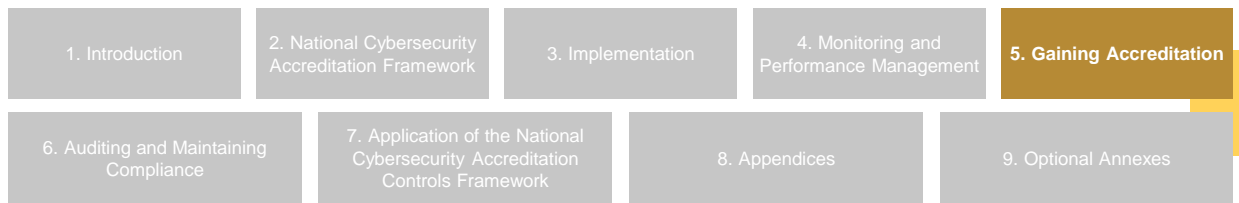


5.4 Voluntary Accreditation Track Process Flowchart



PLEASE NOTE: Entities engaged in voluntary accreditation may wish to engage the services of an Accredited Internal Auditor to assist in the process, this should be done at point 2 if desired.

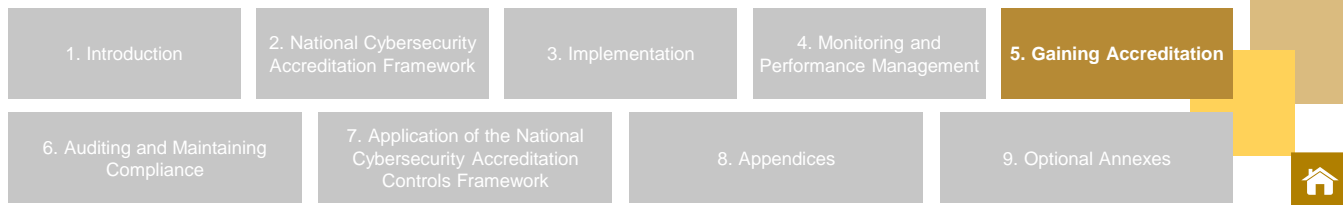




5.5 Maturity Modelling

Entities will have different maturity level requirements, depending on the type of information stored, the information value, the function of the Entity and many other factors. The NCAP Maturity Model establishes a unified method of tracking maturity across Entities. The NCAP Maturity Model does not replace any other organizational requirements but establishes a UAE specific methodology for measuring cyber security maturity. Specific guidance on measuring an Entities maturity will be provided by the National Lead Agency upon application for the accreditation process.

NCAP Maturity Modelling Levels		
Level	Compliance Note	Suitability
I	Minimal or ad-hoc compliance with guiding principles.	Only suitable for Entities that are just beginning to implement cyber security.
II	Basic compliance requirements are met, controls are in place to defend against common, non-targeted attackers.	The minimum compliance level suitable for the majority of non-government Entities.
III	Intermediate level of compliance requirements met - Controls in place to defend against common targeted attackers. The cyber security principles are established as standard business practices and robustly implemented throughout the organization.	The minimum compliance level suitable for the majority of Government Entities.
IV	High level of compliance. Controls in place to defend against many Advanced Persistent Threats. A deliberate focus on optimization and continual improvement exists for the implementation of the cyber security principles throughout the organization.	A higher level of compliance, suitable for Government or Entities dealing with sensitive information.



5.6 Cross Recognition of Existing Accreditation

In some circumstances, an entity seeking either mandatory or voluntary accreditation may hold existing certifications from internationally recognized standards. If this is the case, the NCAP may, at its sole discretion, allow entities that hold existing certifications to attain accreditation without undergoing the full audit process.

For this to occur, entities must provide:

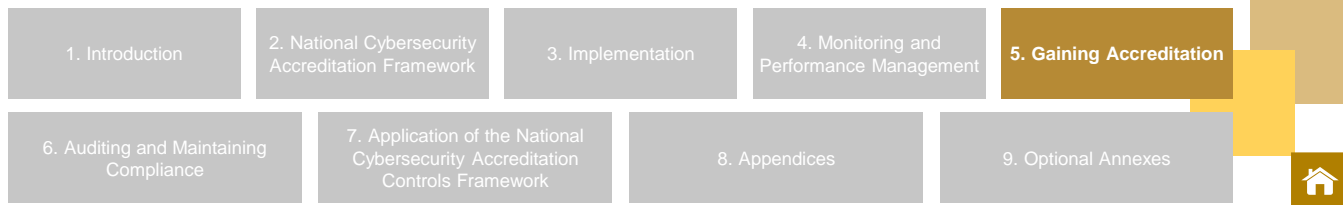
- Formal evidence of the existing certification/accreditation
- Audit documentation that supports the existing certification/accreditation

Additionally, the area or systems that are being NCAP accredited (targets of assessment) must be identical to those that were certified/assessed by the cross-recognized certification/accreditation, and the cross-recognized certification/accreditation must cover all relevant controls from the NCAP.

Existing certifications/accreditations that may be cross-recognized by the NCAP are:

- CREST
- ISO27001
- NIST SP 800-53 REV. 5
- HIPAA
- PCI-DSS





5.6 Cross Recognition of Existing Accreditation

5.6.1 Applying for Cross – Recognition

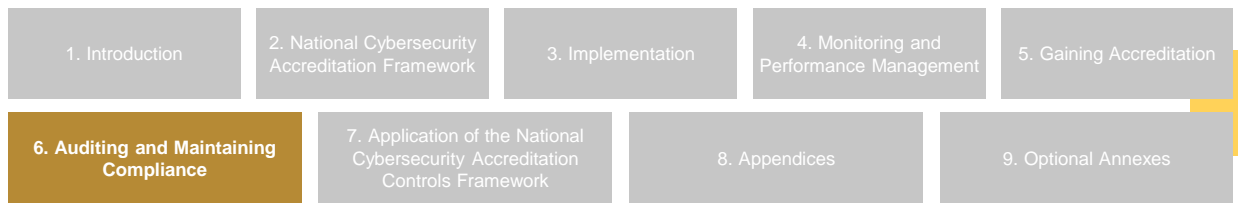
To apply for cross recognition of an existing certification/accreditation, Entities should contact the National Lead Agency directly.

Cross-recognition may also be used to support part of an NCAP accreditation process, i.e., if an Entity is using a service that is certified/accredited using a cross-recognized certification/accreditation, the Entities' service provider can simply provide evidence of the existing certification/accreditation to cover that portion of the system for the assessment.



The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, irregular shapes. The overall color palette is a mix of light beige, olive green, and dark brown. On the right side, there are vertical lines resembling a circuit board or data stream. A large, solid black rectangle is positioned in the lower right quadrant, containing the section title in white and gold text.

SECTION 6
**AUDITING AND
MAINTAINING
COMPLIANCE**



6.1 Audit Process

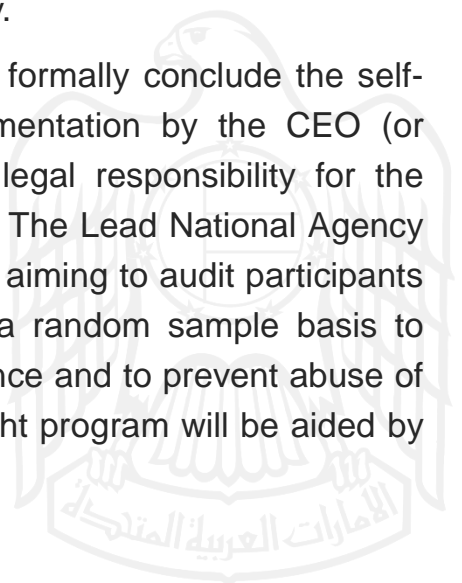
As described in detail in the Framework Model, UAE government and Entities can gain certification under the NCAP through a dual-track system. Mandated entities must participate and their assessment is carried out by the National Lead Agency directly, through an Authorized Government Entity, or through the Independent Assessors Program. Formal accreditation in their case is issued solely by the National Lead Agency. Detailed audit methodology, including scoping guidelines, evidence collection and retention are to be defined by a detailed Standard Operating Procedure documentation published by the Lead National Agency.

An outline for the NCAP Independent Assessors Program, to be implemented by the National Lead Agency, is provided in Annex B.

A full documentation pack for both the mandatory and the voluntary accreditation tracks is available from the National Lead Agency upon registration for the accreditation process.

In a parallel process, as defined in detail in the Framework Model, Entities conducting business in the UAE can get certification under the NCAP through a voluntary process that follows a self-assessment process. Details for such a process are to be defined in overarching Standard Operating Procedure documentation provided by the Lead National Agency.

As defined above, a critically important final step to formally conclude the self-certification process is the signature of the documentation by the CEO (or equivalent) of the private sector entity taking full legal responsibility for the validity and integrity of the self-assessment process. The Lead National Agency shall establish a rigorous external oversight program aiming to audit participants of the voluntary track self-certification process on a random sample basis to provide effective regulatory oversight, quality assurance and to prevent abuse of the program. The implementation of such an oversight program will be aided by the Independent Assessors Program.





6.2 Maintaining Compliance

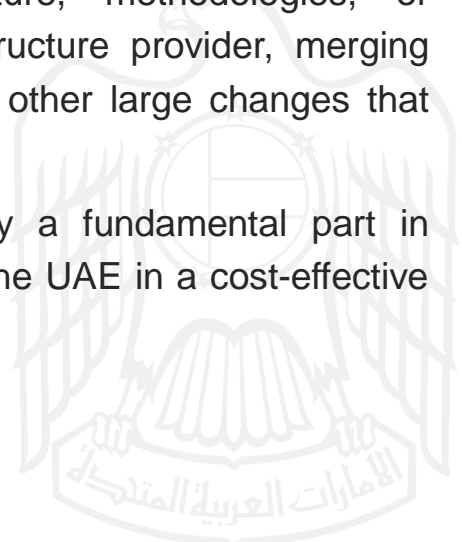
To make sure the NCAP provides relevant assurance to all stakeholders, mandatory track accreditations and certificates issued are to expire after three (3) years. This requirement is necessary as technology and threat environment shifts rapidly and corresponding changes are also reflected in the UAE Information Assurance Regulation. Accordingly, the NCAP must reflect the dynamic nature of the information technology field to provide meaningful assurance for UAE stakeholders.

The mandatory accreditation process must be completed every three (3) years to maintain compliance and in line with changing requirements set forth by the National Lead Agency through regular updates to the National Cyber security Accreditation Controls Framework. Scoping decisions in line with the detailed Standard Operating Procedure documentation published by the Lead National Agency should consider the results of and evidence provided during previous assessments to streamline the process where relevant.

Voluntary track certification must be undertaken on an annual basis.

Re-accreditation under the NCAP should also be undertaken if there is a significant change to technology infrastructure, methodologies, or processes (such as moving to another infrastructure provider, merging departments or company technology stacks, or other large changes that impact organizational security profiles).

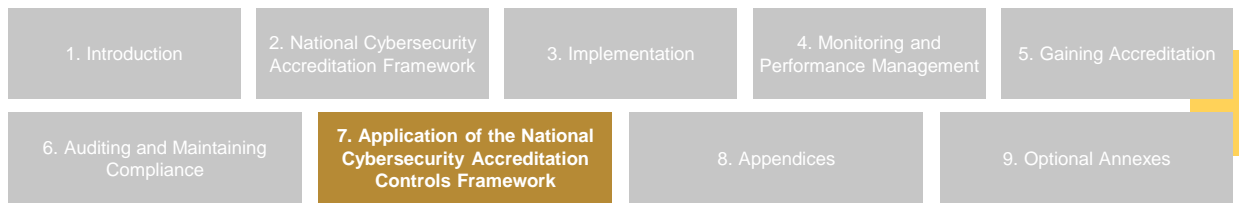
The Independent Assessors Program will play a fundamental part in carrying out compliance maintenance efforts in the UAE in a cost-effective way.





SECTION 7

APPLICATION OF THE NATIONAL CYBER SECURITY ACCREDITATION CONTROLS FRAMEWORK



The National Cybersecurity Accreditation Controls Framework is provided in Annex C.

7.1 Governance

The National Cyber security Accreditation Controls Framework is an essential element of the UAE NCAP and thus owned by the National Lead Agency. To make sure it is kept up-to-date and reflects changes and shifts in the rapidly changing technology and threat environment, it must be reviewed at least on an annual basis. The National Cyber security Accreditation Controls Framework of the UAE NCAP is based on and to be kept in line with the UAE Information Assurance Regulation.






The National Cybersecurity Accreditation Controls Framework is provided in Annex C.

7.2 Applicability of Controls

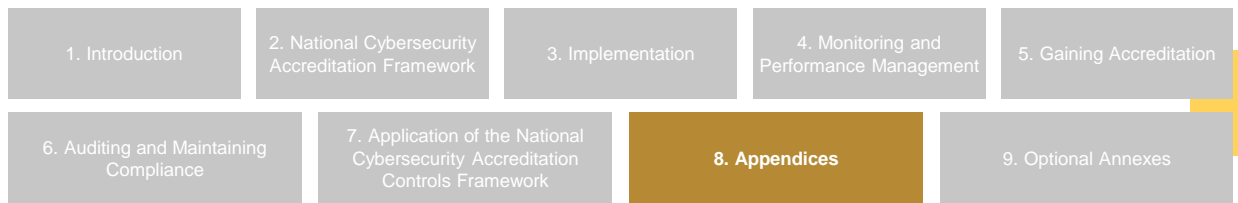
Most controls listed in the National Cyber security Accreditation Controls Framework of the UAE NCAP are mandatory ('always applicable') to ensure a common cyber security baseline throughout the UAE cyber ecosystem. As described, the National Cyber security Accreditation Controls Framework is based on the UAE Information Assurance Regulation reflecting common risk profiles of entities.

A subset of controls however is optional (as indicated) to allow individual scoping decisions to be made based on the risk profile of the assessed entity reflecting their specific IT environments and risk assessments considering their business and operational context. These optional controls play an important role in treating entity specific risks and should be leveraged accordingly and in line with industry best practice.



The background features a complex network of thin, light-colored lines connecting various nodes. Some nodes are represented by small circles, while others are larger, elongated ovals. The overall color palette is a mix of light beige, olive green, and dark brown. On the right side, there are vertical lines resembling a circuit board or data stream, with small circles at various intervals. A large, solid black rectangle is positioned in the lower-left to center area, serving as a backdrop for the text.

SECTION 8
APPENDICES



8.1 Annex A: Reference Documents – UAE Policies and Standards¹

UAE National Cybersecurity Strategy

Core strategy document that defines cybersecurity vision, aspirations, strategic pillars for programmatic implementation, regulatory objectives and requirements and envision capabilities for the United Arab Emirates' cyber ecosystem.

Critical Information Infrastructure Protection Policy (CIIP)

Outlines the activities the CIIP Program will use to identify critical infrastructure sectors and National services; identify the information infrastructures supporting critical National services; and raise the security levels of those information infrastructures by implementing mandatory cybersecurity standards and requirements.

National Information Assurance Framework (NIAF) and Information Assurance Standards (IA)

Outlines the guidelines necessary to raise the minimum cybersecurity levels across all UAE entities by helping to build a common understanding of Information Assurance (IA) requirements at the entity level and raise information infrastructure security levels that support critical National services through the integration of individual entities into a sector and National context.

National Cyber Risk Management Framework (NCRMF)

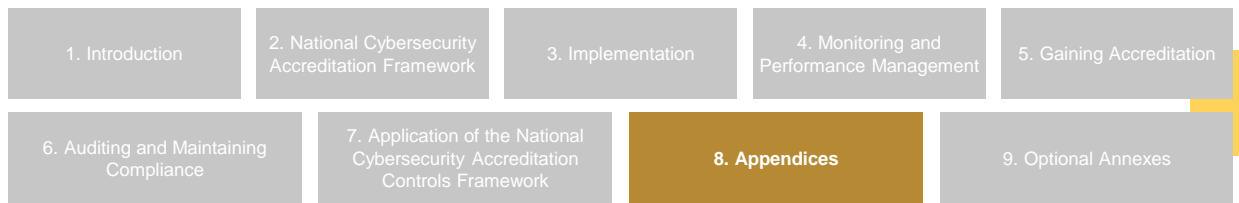
Defines the National approach and methodology to identify, evaluate, and treat cybersecurity risks for CII.

National Cyber Information Sharing Policy (NCIS)

The National Cyber Information Sharing policy outlines key requirements for inter-entity and inter-sector communication that serves as a key input to developing National situational awareness.

Cyber Security Standards issued by the Cyber Security Council by Cabinet Resolution No. (8/8 and) for the year 2021

The cybersecurity standards define the main requirements to raise the level of cybersecurity of the entities and institutions operating in the country and to develop the level of cybersecurity at the national level.

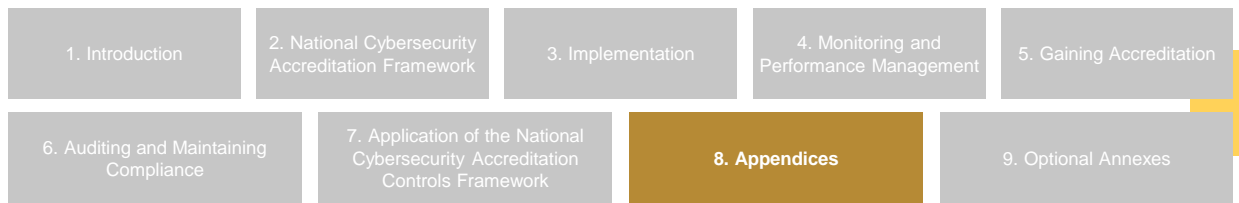


8.2 Annex B: Outline of an Independent Assessors Program

The National Lead Agency will establish an Independent Assessors Program (IAP) as a flexible and resource-efficient approach to extend its services in rolling out and subsequently maintaining the program. The IAP allows for the inclusion of vetted, qualified professional organizations with the necessary skills and resources to attest conformity of UAE entities with NCAP requirements. This allows the National Lead Agency to leverage private sector resources for the successful implementation of the NCAP following a force-multiplier model. Qualified assessors participating in the IAP Program will also contribute to the stability and security of UAE cyberspace by promoting the implementation of higher cyber security standards across the UAE cyber ecosystem.

Additionally, the National Lead Agency may appoint Authorized Government Entities that are authorized to carry out audits and attestation on behalf of the National Lead Agency. Authorized Government Entities must comply with NCAP requirements, and individual staff supervising audits within Authorized Government Entities must meet the same requirements outlined for Independent Authorized Assessors (below). A list of Authorized Government Entities shall be published and maintained by the National Lead Agency.



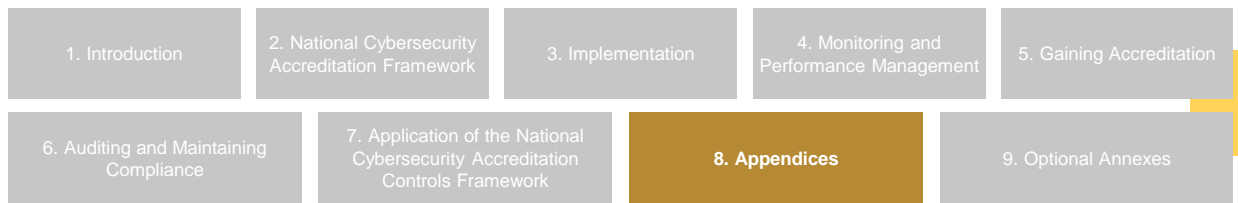


8.2 Annex B: Outline of an Independent Assessors Program

Assessors participating in the IAP may both assist in carrying out or validating assessments for entities of the Mandatory track and they can provide additional services or implement assessments for entities of the Voluntary track. Specific SOPs are to be prepared by the National Lead Agency to regulate and define the details of these services, including the requirements for implementing assessments (incl. general requirements for qualification, scoping rules, evidence collection and retention, confidentiality, liaison with the National Lead Agency, etc.).

The National Lead Agency shall establish a detailed standard or SOP defining criteria, standards, approaches to testing, data security, subcontracting and relevant procedures (including questioners, etc.) for Assessors of the Program. Cyber security service providers who wish to participate in the Independent Assessors Program must go through a proper selection process aiming to ensure quality control and consistency over the implementation of the Program. The overall process is to ensure that participating Assessors demonstrate their bona fides, capabilities and competencies necessary to deliver on the requirements of the IAP. Specific requirements shall be made publicly available and prospective Assessors are to be encouraged to make sure they comply with them prior to submitting their application.





8.2 Annex B: Outline of an Independent Assessors Program

Applicants applying for a license are to be provided with an NDA by the National Lead Agency to safeguard to confidentiality of the application process. An application fee can be considered and its proceeds can be leveraged to cover the cost of the evaluation process.

Approved Assessors shall be required to renew their license regularly (every one or two years).

Those successfully getting licensed as Assessors of the IAP will be listed in an official database maintained and published by the Lead National Agency available to the public. The Lead National Agency in turn is to clearly articulate that only licensed IAP Assessors are to be hired by members of the UAE cyber ecosystem who wish to get accredited.

To ensure provision of high-quality services and accountability, only individuals should be certified under the IAP, as a minimum requirement individuals should hold and maintain a current industry qualification from the list below, and have at least 5 years of relevant, verifiable experience.

Certifications

CISM - Certified Information Security Manager (ISACA)

CISSP - Certified Information System Security Professional (ISC2)

CISA - Certified Information System Auditor (ISACA)

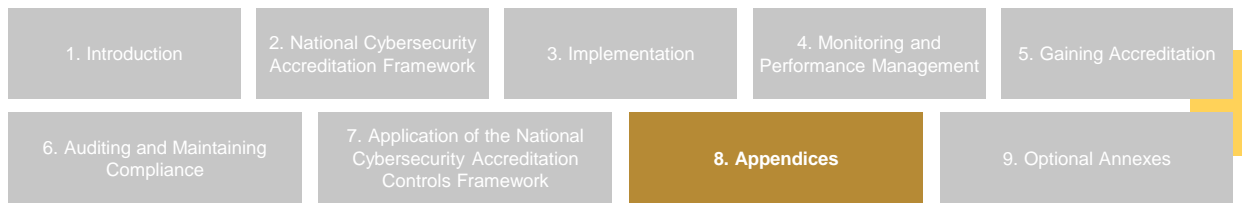
CRISC - Certified Risk and Information System Control (ISACA)

GSNA - GIAC System and Network Auditor (SANS)

ISO 27001 Lead Auditor (Global Association for Quality Management)

PCI QSA (PCI Security Standards Council)





8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

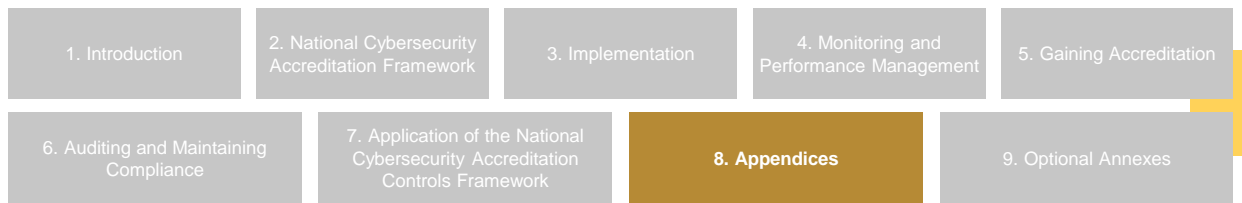
The UAE National Cyber security Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation². A full documentation pack for Entities seeking accreditation is available from the National Lead Agency upon initial application for the accreditation process.

Governance Controls

8.3.1 M1 Strategy and Planning

M1	Strategy and Planning
M1.1	Entity Context and Leadership
M1.1.1	Understanding the Entity and its Context
M1.1.2	Leadership and Management Commitment
M1.1.3	Roles and Responsibilities for Information Security
M1.2	Information Security Policy
M1.2.1	Information Security Policy
M1.2.2	Supporting Policies for Information Security
M1.3	Organization of Information Security
M1.3.1	Authorization Process for Information System
M1.3.2	Confidentiality Agreements
M1.3.3	Contact with Authorities
M1.3.5	Identification of Risks Related to External Parties
M1.3.7	Addressing Security in Third Party Agreements
M1.4	Support (Resourcing)
M1.4.1	Providing Necessary Resources
M1.4.2	Internal and External Communication
M1.4.3	Documentation

²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

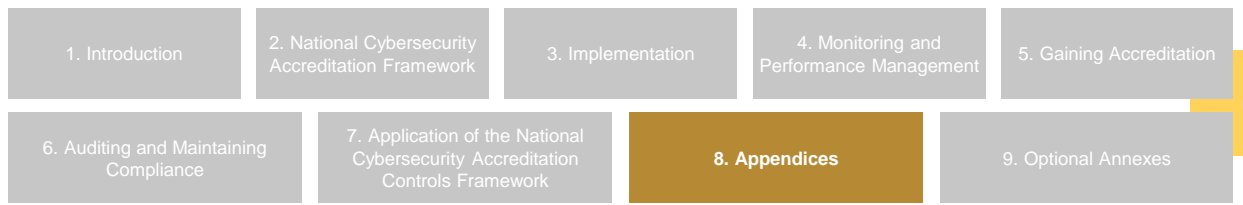
Governance Controls

8.3.2 M2 Information Security Risk Management

M2	Information Security Risk Management
M2.1	Information Security Risk Management Policy
M2.1.1	Information Security Risk Management Policy
M2.2	Information Security Risk Assessment
M2.2.1	Information Security Risk Identification
M2.2.2	Information Security Risk Analysis
M2.2.3	Information Security Risk Evaluation
M2.3	Information Security Risk Treatment
M2.3.1	Information Security Risk Treatment Options
M2.3.2	Identification of Controls
M2.3.3	Risk Treatment Plan



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

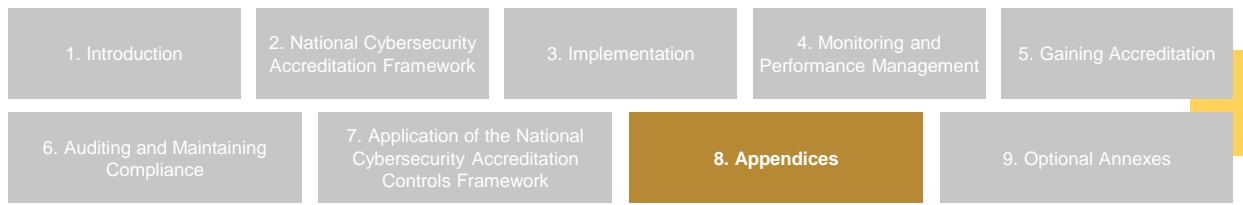
Governance Controls

8.3.3 M3 Awareness and Training

M3	Awareness and Training
M3.1	Awareness and Training Policy
M3.1.1	Awareness and Training Policy
M3.2	Awareness and Training Planning
M3.2.1	Awareness and Training Program
M3.3.3	Training Execution
M3.4	Security Awareness
M3.4.1	Awareness Campaign



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

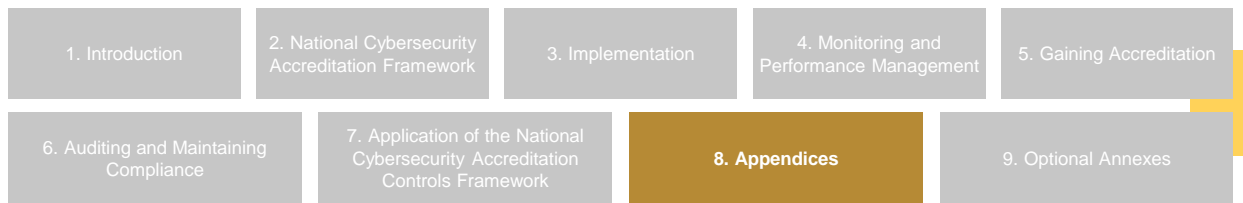
Governance Controls

8.3.4 M4 Human Resources Security

M4	Human Resources Security
M4.1	Human Resources Security Policy
M4.1.1	Human Resources Security Policy
M4.2	Human Security Prior to Employment
M4.2.1	Screening
M4.2.2	Terms and Conditions of Employment
M4.3	During Employment
M4.3.1	Management Responsibilities
M4.3.2	Disciplinary Process
M4.4	Termination or Change of Employment
M4.4.1	Termination Responsibilities
M4.4.2	Return of Assets
M4.4.3	Removal of Access Rights



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

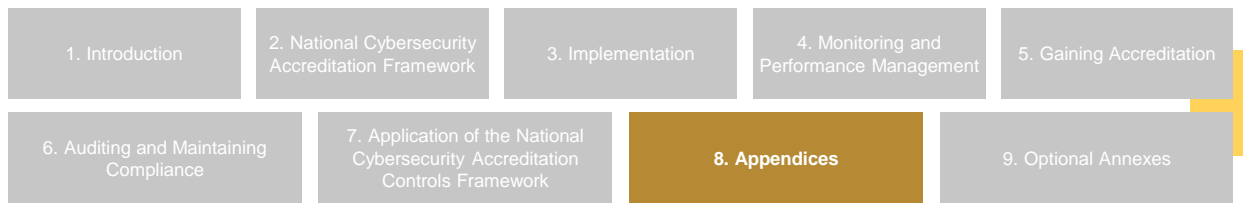
Governance Controls

8.3.5 M5 Compliance

M5	Compliance
M5.1	Compliance Policy
M5.1.1	Compliance Policy
M5.2	Compliance with Information Security Legal Requirements
M5.2.1	Identification of Applicable Legislation
M5.2.2	Protection of Organizational Records
M5.2.3	Data Protection and Privacy of Personal Information
M5.2.4	Regulation of Cryptographic Controls



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

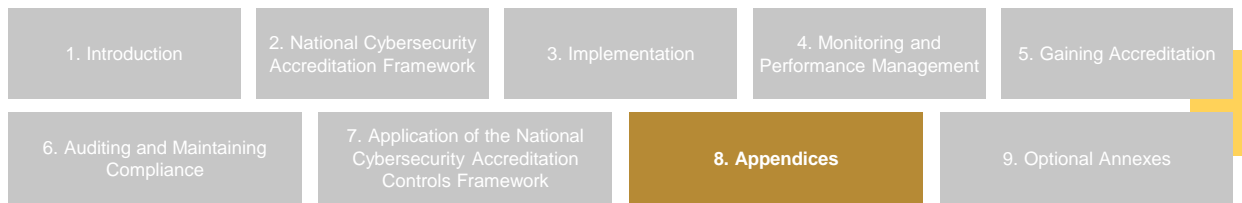
Governance Controls

8.3.6 M6 Performance Evaluation and Improvement

M6	Performance Evaluation and Improvement
M6.1	Performance Evaluation Policy
M6.1.1	Performance Evaluation Policy
M6.2.1	Monitoring, Measurement, Analysis and Evaluation
M6.2.2	Internal Audits
M6.3.1	Corrective Action
M6.3.2	Continuous Improvement



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

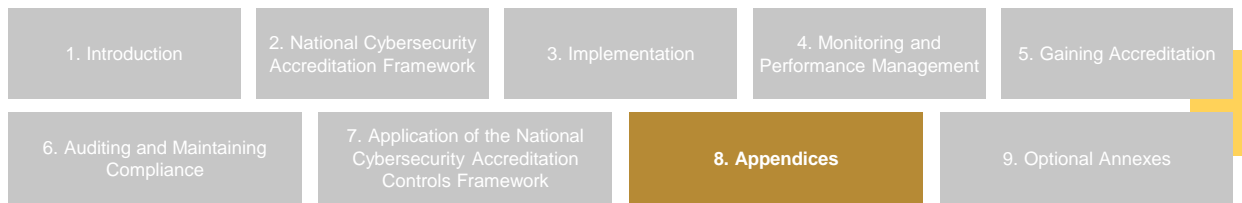
Technical Controls

8.3.7 T1 Asset Management

T1	Asset Management
T1.1	Asset Management Policy
T1.1.1	Asset Management Policy
T1.2	Responsibility for Assets
T1.2.1	Inventory of Assets
T1.2.2	Ownership of Assets
T1.2.3	Acceptable Use of Assets
T1.2.4	Acceptable Bring Your Own, Device Arrangements
T1.3	Information Classification
T1.3.1	Classification of Information
T1.3.2	Labeling of Information
T1.3.3	Handling of Information Assets
T1.4	Media Handling
T1.4.1	Management of Removable Media
T1.4.2	Disposal of Media

²Version 1.1, published in March, 2020.





8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

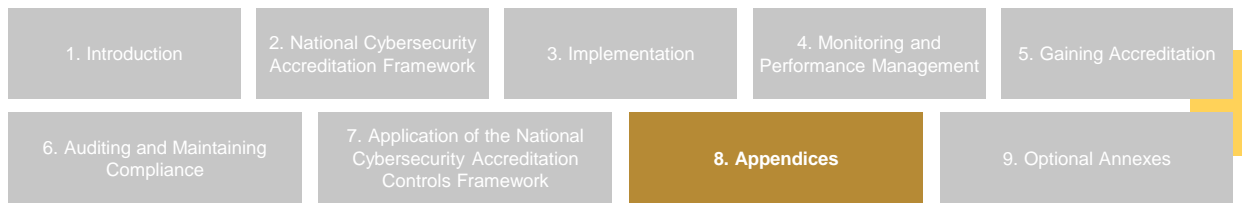
Technical Controls

8.3.8 T2 Physical and Environmental Security

T2	Physical and Environmental Security
T2.1	Physical and Environmental Security Policy
T2.1.1	Physical and Environmental Security Policy
T2.2	Secure Areas
T2.2.1	Physical Security Perimeter
T2.2.2	Physical Entry Controls
T2.2.4	Protecting Against External and Environmental Threats
T2.2.5 (Optional control - based on risk assessment)	Working in Secure Areas
T2.2.6 (Optional control - based on risk assessment)	Public Access, Delivery and Loading Areas
T2.3	Equipment Security
T2.3.1	Equipment Siting and Protection
T2.3.2	Supporting Utilities

²Version 1.1, published in March, 2020.





8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

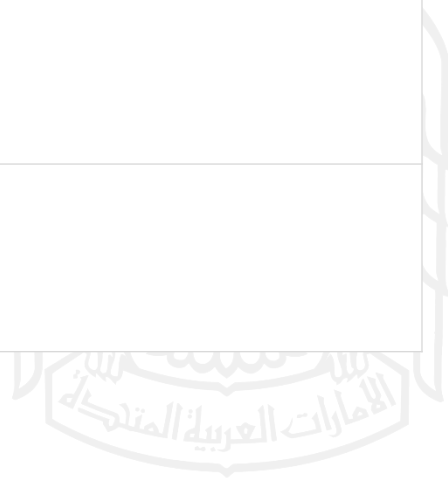
The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

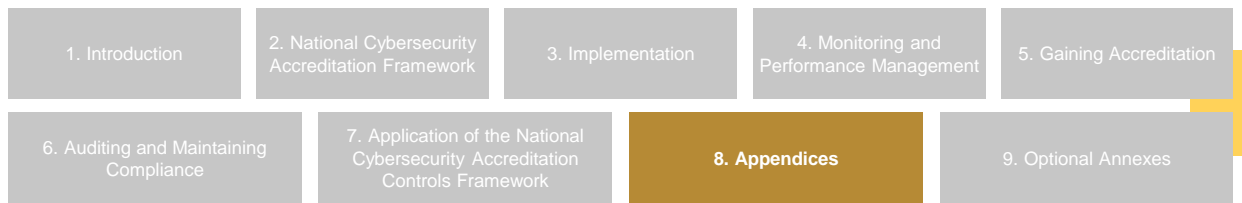
Technical Controls

8.3.8 T2 Physical and Environmental Security

T2	Physical and Environmental Security
T2.3.3 (Optional control - based on risk assessment)	Cabling Security
T2.3.4 (Optional control - based on risk assessment)	Equipment Maintenance
T2.3.5 (Optional control - based on risk assessment)	Security of Equipment Off-Premise
T2.3.6	Secure Disposal or Re-Use of Equipment
T2.3.8 (Optional control - based on risk assessment)	Unattended User Equipment
T2.3.9 (Optional control - based on risk assessment)	Clear Desk and Clear Screen Policy

²Version 1.1, published in March, 2020.





8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

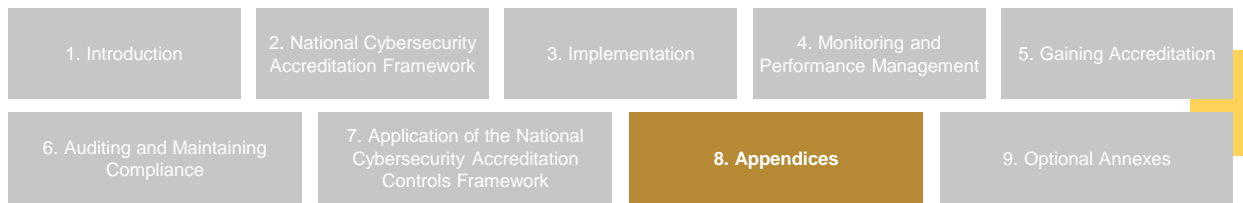
Technical Controls

8.3.9 T3 Operations Management

T3	Operations Management
T3.1	Operations Management Policy
T3.1.1	Operations Management Policy
T3.2	Operational Procedures and Responsibilities
T3.2.1	Common System Configuration Guidelines
T3.2.2	Documented Operating Procedures
T3.2.3	Change Management
T3.2.4	Segregation of Duties
T3.2.5	Separation of Development, Test and Operational Environments
T3.3	System Planning and Acceptance
T3.3.1 (Optional control - based on risk assessment)	Capacity Management
T3.3.2	System Acceptance and Testing
T3.4	Protection From Malware
T3.4.1	Controls Against Malware

²Version 1.1, published in March, 2020.





8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

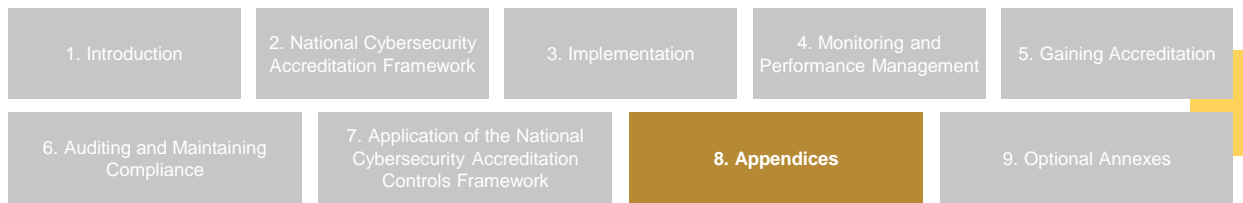
Technical Controls

8.3.9 T3 Operations Management

T3	Operations Management
T3.5	Backup
T3.5.1	Information Backup
T3.6	Monitoring
T3.6.1	Monitoring Policy and Procedures
T3.6.2	Audit Logging
T3.6.3	Monitoring System Use
T3.6.4	Protection of Log Information
T3.6.5	Administrator and Operator Logs (Privileged Accounts)
T3.6.6	Fault Logging
T3.6.7	Clock Synchronization



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

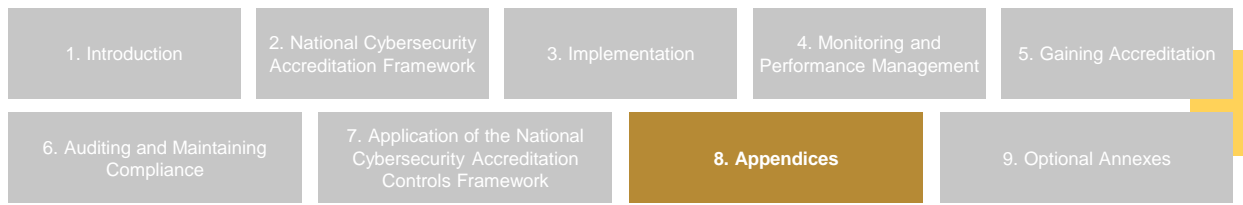
Technical Controls

8.3.10 T4 Communication

T4	Communication
T4.1	Communications Policy
T4.1.1	Communications Policy
T4.2	Information Transfer
T4.2.1	Information Transfer Procedures
T4.2.2	Agreements on Information Transfer
T4.2.3 (Optional control - based on risk assessment)	Physical Media in Transit
T4.2.4	Electronic Messaging
T4.2.5 (Optional control - based on risk assessment)	Business Information System



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

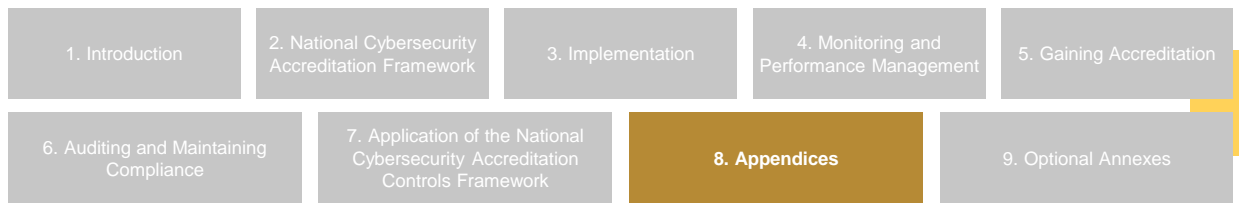
Technical Controls

8.3.10 T4 Communication

T4	Communication
T4.3 (Optional control - based on risk assessment)	Electronic Commerce Services
T4.3.1 (Optional control - based on risk assessment)	Electronic Commerce
T4.3.2 (Optional control - based on risk assessment)	On-Line Transactions



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

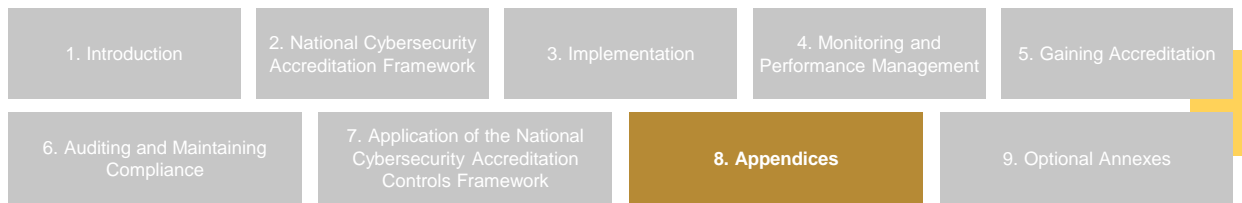
Technical Controls

8.3.10 T4 Communication

T4	Communication
T4.4 (Optional control - based on risk assessment)	Information Sharing Protection
T4.4.1 (Optional control - based on risk assessment)	Connectivity to Information Sharing Platforms
T4.4.2	Information Released into Information Sharing Communities
T4.5	Network Security Management
T4.5.1	Network Controls
T4.5.2	Security of Network Services
T4.5.4	Security of Wireless Networks



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

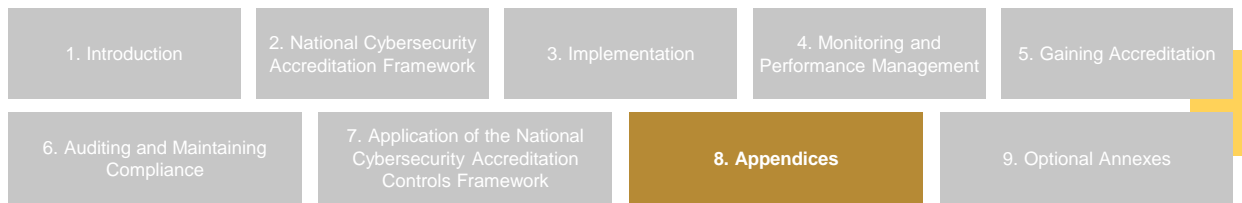
Technical Controls

8.3.11 T5 Access Control

T5	Access Control
T5.1	Access Control Policy
T5.1.1	Access Control Policy
T5.2	User Access Management
T5.2.1	User Registration
T5.2.2	Privilege Management
T5.2.3	User Security Credentials Management
T5.2.4 (Optional control - based on risk assessment)	Review of User Access Rights
T5.3	User Responsibilities (Acceptable Use Policy)
T5.3.1	Use of Security Credentials
T5.4	Network Access Control
T5.4.1	Policy on Use of Network Services



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

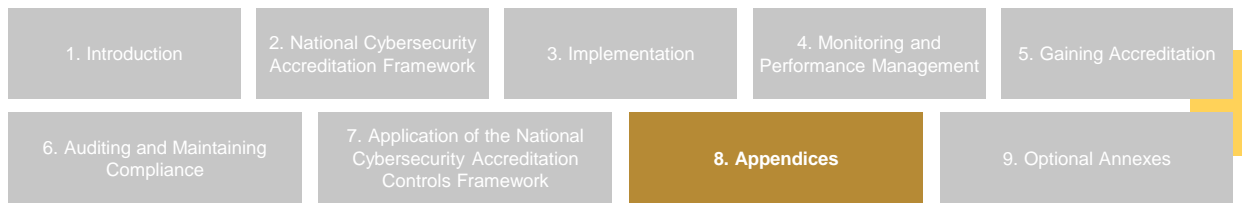
Technical Controls

8.3.11 T5 Access Control

T5	Access Control
T5.4.2 (Optional control - based on risk assessment)	User Authentication for External Connections
T5.4.3	Equipment Identification in Networks
T5.4.4	Remote Diagnostic and Configuration Protection
T5.4.5	Network Connection Control
T5.4.6	Network Routing Control
T5.4.7	Wireless Access
T5.5	Operating System Access Control
T5.5.1	Secure Log-On Procedures
T5.5.2	User Identification and Authentication
T5.5.3	User Credentials Management System
T5.5.4	Use of System Utilities
T5.6	Application and Information Access Control
T5.6.1	Information Access Restriction

²Version 1.1, published in March, 2020.





8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

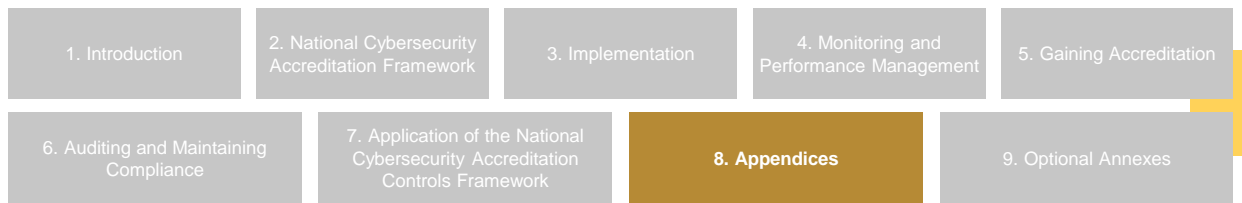
Technical Controls

8.3.12 T6 Third-Party Security

T6	Third-Party Security
T6.1	Third Party Security Policy
T6.1.1	Third Party Security Policy
T6.2	Third Party Service Delivery Management
T6.2.1	Service Delivery
T6.2.2 (Optional control - based on risk assessment)	Monitoring and Review of Third Party Services
T6.2.3	Managing Changes to Third Party Services
T6.3	Cloud Computing
T6.3.1	Information Security Requirements for Cloud Environments
T6.3.2	Service Delivery Agreements with Cloud Providers



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

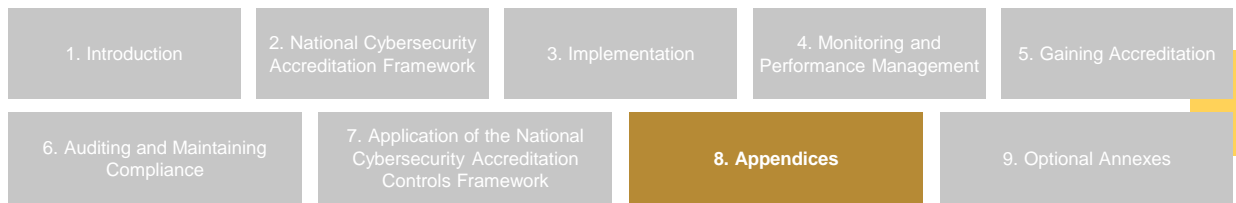
Technical Controls

8.3.13 T7 Information System Acquisition, Development and Maintenance

T7	Information System Acquisition, Development and Maintenance
T7.1	Information System Acquisition, Development and Maintenance Policy
T7.1.1	Information System Acquisition, Development and Maintenance Policy
T7.2	Security Requirements of Information System
T7.2.1	Security Requirements Analysis and Specification
T7.3 (Optional control - based on risk assessment)	Correct Processing in Applications
T7.3.1 (Optional control - based on risk assessment)	Input Data Validation



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

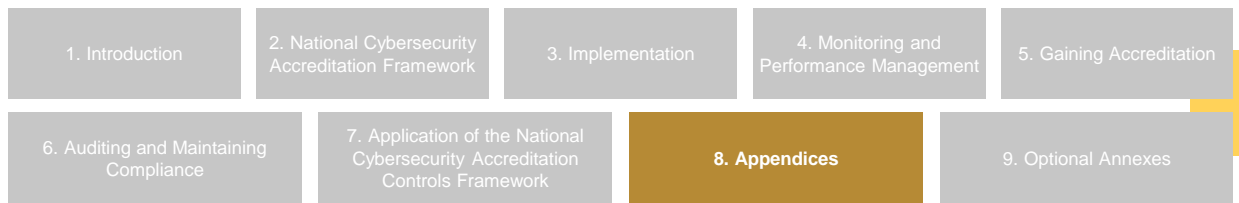
Technical Controls

8.3.13 T7 Information System Acquisition, Development and Maintenance

T7	Information System Acquisition, Development and Maintenance
T7.3.2 (Optional control - based on risk assessment)	Control of Internal Processing
T7.3.3 (Optional control - based on risk assessment)	Message Integrity
T7.3.4 (Optional control - based on risk assessment)	Output Data Validation
T7.4	Cryptographic controls
T7.4.1	Policy on the Use of Cryptographic Controls



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

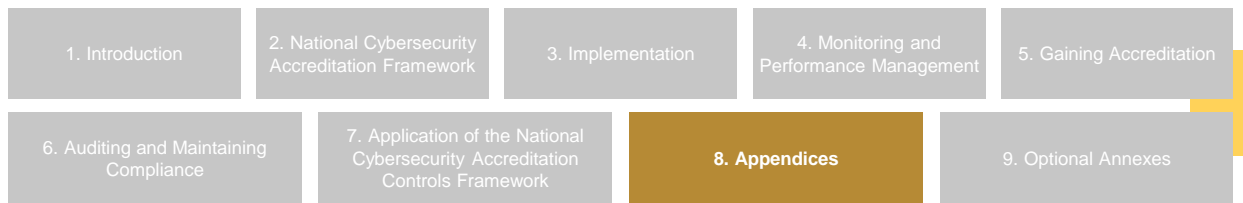
Technical Controls

8.3.13 T7 Information System Acquisition, Development and Maintenance

T7	Information System Acquisition, Development and Maintenance
T7.4.2	Key Management
T7.5	Security of System Files
T7.5.1	Control of Operational Software [Production environment]
T7.5.2	Protection of System Test Data
T7.5.3 (Optional control - based on risk assessment)	Access Control to Program Source Code
T7.6	Security in Development and Support Processes
T7.6.1	Change Control Procedures
T7.6.2	Technical Review of Applications After Operating System Changes
T7.6.3	Restrictions on Changes to Software Packages
T7.6.4	Information Leakage



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

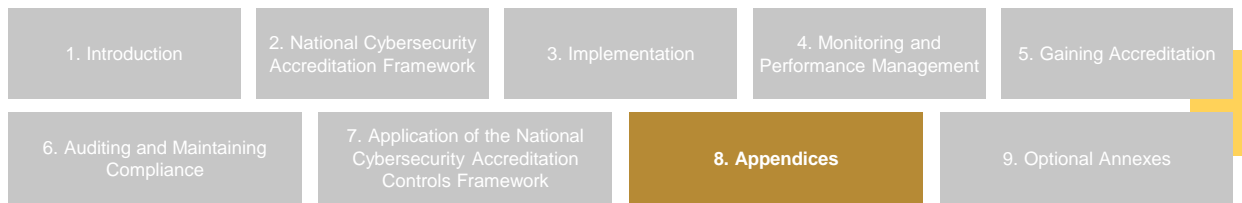
Technical Controls

8.3.13 T7 Information System Acquisition, Development and Maintenance

T7	Information System Acquisition, Development and Maintenance
T7.6.5 (Optional control - based on risk assessment)	Outsourced Software Development
T7.7	Technical Vulnerability Management
T7.7.1	Control of Technical Vulnerabilities
T7.8	Supply Chain Management
T7.8.1	Supply Chain Protection Strategy
T7.8.2	Supplier Reviews
T7.8.3	Limitation of Harm
T7.8.4	Supply Chain Operations Security
T7.8.6	Processes to Address Weaknesses or Deficiencies
T7.8.7	Supply of Critical Information System Components



²Version 1.1, published in March, 2020.



8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

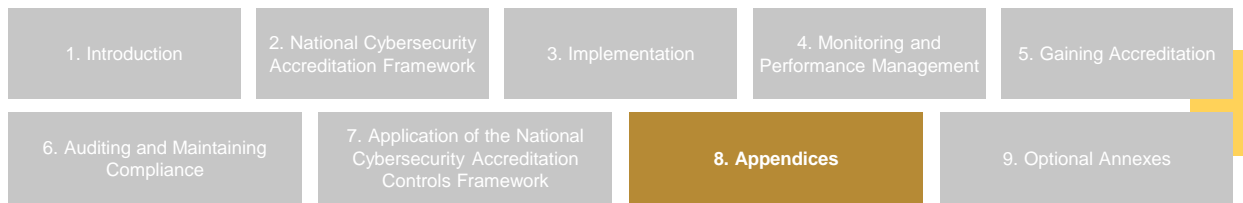
Technical Controls

8.3.13.1 T8 Information Security Incident Management

T8	Information Security Incident Management
T8.1	Information Security Incident Management Policy
T8.1.1	Information Security Incident Management Policy
T8.2	Management of Information Security Incidents and Improvements
T8.2.1	Incident Response Plan
T8.2.2	Computer Security Incident Response Team
T8.2.4	Incident Response Training
T8.2.5	Incident Response Testing
T8.2.6 (Optional control - based on risk assessment)	Incident Response Assistance
T8.2.7	Information Security Incident Documentation
T8.2.8	Learning From Information Security Incidents
T8.2.9	Collection of Evidence
T8.3	Information Security Events and Weaknesses Reporting
T8.3.1	Situational Awareness
T8.3.2	Reporting Information Security Events

²Version 1.1, published in March, 2020.





8.3 Annex C: National Cybersecurity Accreditation Controls Framework – Controls List

The UAE National Cybersecurity Accreditation Controls Framework is aligned to the UAE Information Assurance Regulation².

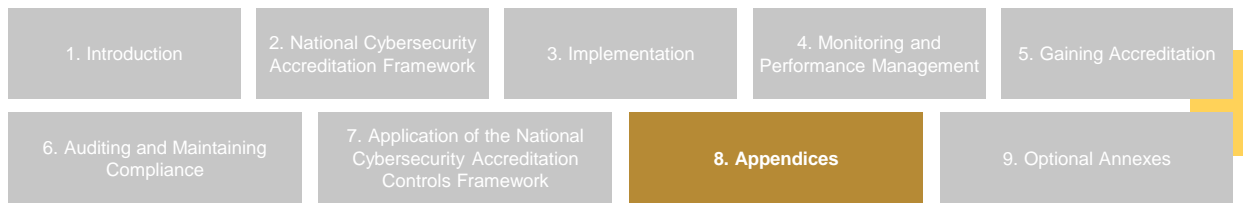
Technical Controls

8.3.14 T9 Information System Continuity Management

T9	Information System Continuity Management
T9.1	Information System Continuity Management Policy
T9.1.1	Information System Continuity Planning Policy
T9.2	Information Security Aspects of Information Continuity Management
T9.2.1	Developing Information System Continuity Plans
T9.2.2	Implementing Information System Continuity Plans
T9.3	Testing, Maintaining and Reassessing Plans
T9.3.1	Testing, Maintaining and Re-Assessing Information System Continuity Plans



²Version 1.1, published in March, 2020.



8.4 Annex D: Abbreviations

Usage	Description
CIIP	UAE Critical Information Infrastructure Protection Policy
CIRT	Computer Security Incident Response Team
CSC	Cyber Security Council of the UAE
IAP	Independent Assessors Program
IA	UAE Information Assurance Regulation
NCAP	National Cybersecurity Accreditation Program
NDA	Non-Disclosure Agreement
NSOC	National (cyber) Security Operations Center
SOC	Security Operations Center
SOP	Standard Operating Procedure

