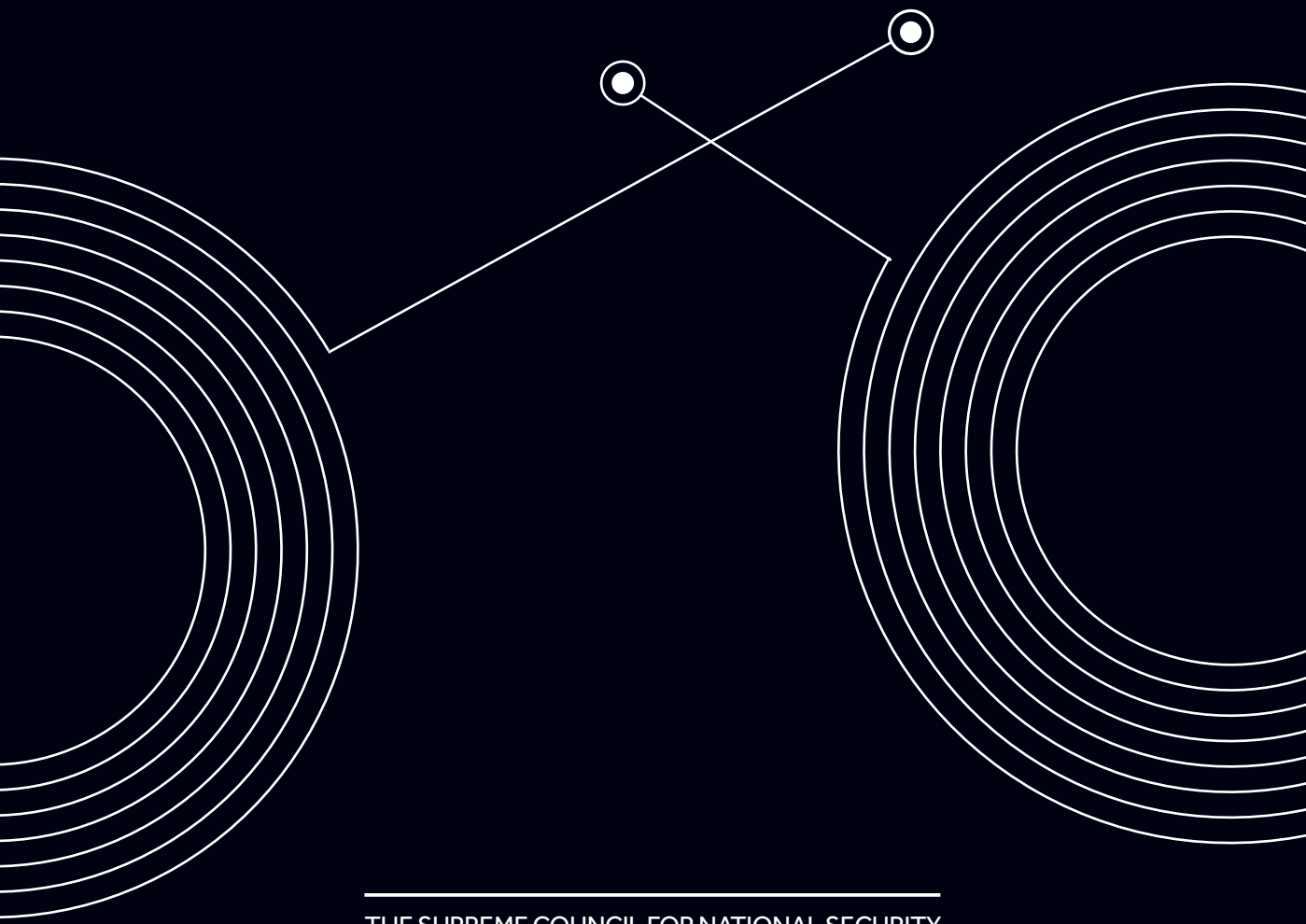
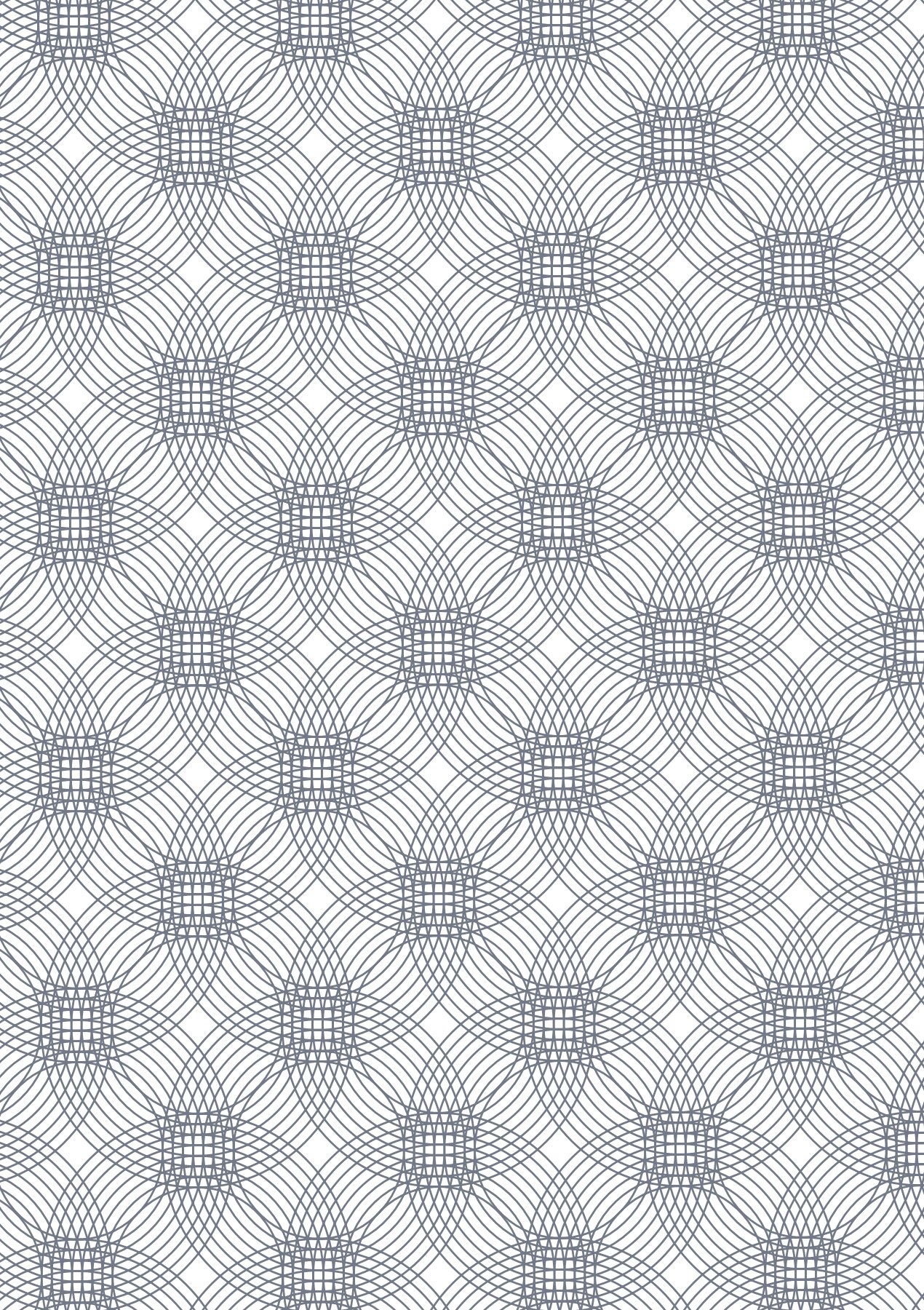
الهيئة الوطنية للأمن الإلكتروني
NATIONAL ELECTRONIC SECURITY AUTHORITY
UNITED ARAB EMIRATES الإمارات العربية المتحدة

THE NATIONAL INFORMATION ASSURANCE FRAMEWORK



THE SUPREME COUNCIL FOR NATIONAL SECURITY

CONTENTS



FOREWORD

The increased adoption of Information Technology (IT), electronic communications, and cyberspace – comprising a global network of interdependent information technology infrastructures, telecommunications networks, and computer processing systems – has provided organizations in the UAE with a platform for delivering innovative services and stimulating economic development, as well as facilitating collaboration and communications among individuals. Our dependence on these technologies will continue to grow in the future, and therefore, the UAE Government is committed to the development of a secure national information and communications infrastructure for UAE organizations and individuals to realize the full potential of its benefits, in the face of an evolving set of related cyber threats.

As cyber threats such as hacktivism and cybercrime evolve, so must our efforts to defend against them in a coordinated and systematic manner. To align and direct national cybersecurity efforts, the UAE Government created the National Electronic Security Authority (NESA) to improve our national cybersecurity, and protect our national information and communications infrastructure. As part of this mandate, NESA developed the UAE Information Assurance (IA) Standards to provide requirements for raising the minimum level of IA across all relevant entities in the UAE.

The adoption of these Standards by UAE entities will sustain the benefits of a trusted digital environment for businesses and individuals across the nation. As cybersecurity is the shared responsibility of every organization and individual, collaboration and partnerships between the Government and private sector organizations are key to success. I am confident that our combined efforts will make great strides in achieving the UAE's national cybersecurity objectives and allow our nation's interests to thrive.

Jassem Bu Ataba Al Zaabi
Director General
National Electronic Security Authority

CHAPTER 01

INTRODUCTION

1.1
PURPOSE OF THE DOCUMENT

As the custodian of a safe and secure nation, the UAE government aims to address cybersecurity challenges. The goal is to ensure the security of national cyberspace in order to foster trust and confidence in the UAE's digital and information environment and to promote economic growth. In accordance with the Federal Law No. 3 of 2012 (and as amended) the UAE government has therefore created the National Electronic Security Authority (NESA) with the mission to enhance the UAE's national security by improving the protection of its Information and Communication Technologies (ICT) infrastructure through world-class technical and regulatory capabilities, human capital and increasing public awareness.

The UAE National Cyber Security Strategy (NCSS), developed and governed by NESA, sets the course for the government's ongoing commitment to protect national cyberspace. It outlines the strategic areas of focus required to sustain national cybersecurity, and the specific objectives within each focus area and a roadmap to achieve these objectives.

The UAE National Information Assurance Framework (NIAF) described herein supports the implementation of the NCSS. The purpose of this NIAF is to outline for stakeholders the NIAF components that aim to accomplish two core objectives:

- **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**
- **Raise information infrastructure security levels that support critical national services through the integration of individual entities into a sector and national context**

1.2
PRINCIPLES OF INFORMATION ASSURANCE

Information Assurance (IA) is the practice of protecting information and managing risks and continuity related to the use, processing, storage, and transmission of information or data, and the systems and processes used for those purposes.

While focused primarily on information in electronic form, the full range of IA also encompasses physical forms of information. The aim is to assure, to the extent possible, securing information in any form in a manner commensurate to its criticality and value.

The Information Assurance is a superset of information security; it covers a much broader range of information protection and management aspects including business/information continuity, disaster recovery, compliance, certification, and accreditation, etc.

The five key principles of Information Assurance are:

1.2.1 CONFIDENTIALITY

Confidentiality ensures that information is accessible only to those authorized to have access, and that it is not made available or disclosed to unauthorized entities. It requires those who hold, process or transmit information to be diligent in preventing intentional or accidental security breaches.

1.2.2 INTEGRITY

Integrity ensures that changes to information cannot be executed without detection.

1.2.3 AVAILABILITY

Availability ensures that an information asset is accessible and usable when needed by an authorized entity. In this context, information assets include data, systems, facilities, networks, and computers.

1.2.4 AUTHENTICATION

Authentication is the process of determining whether the claim of identity made by an entity is true or not. During authentication, an entity presents its credentials, which are then validated against stored credential information.

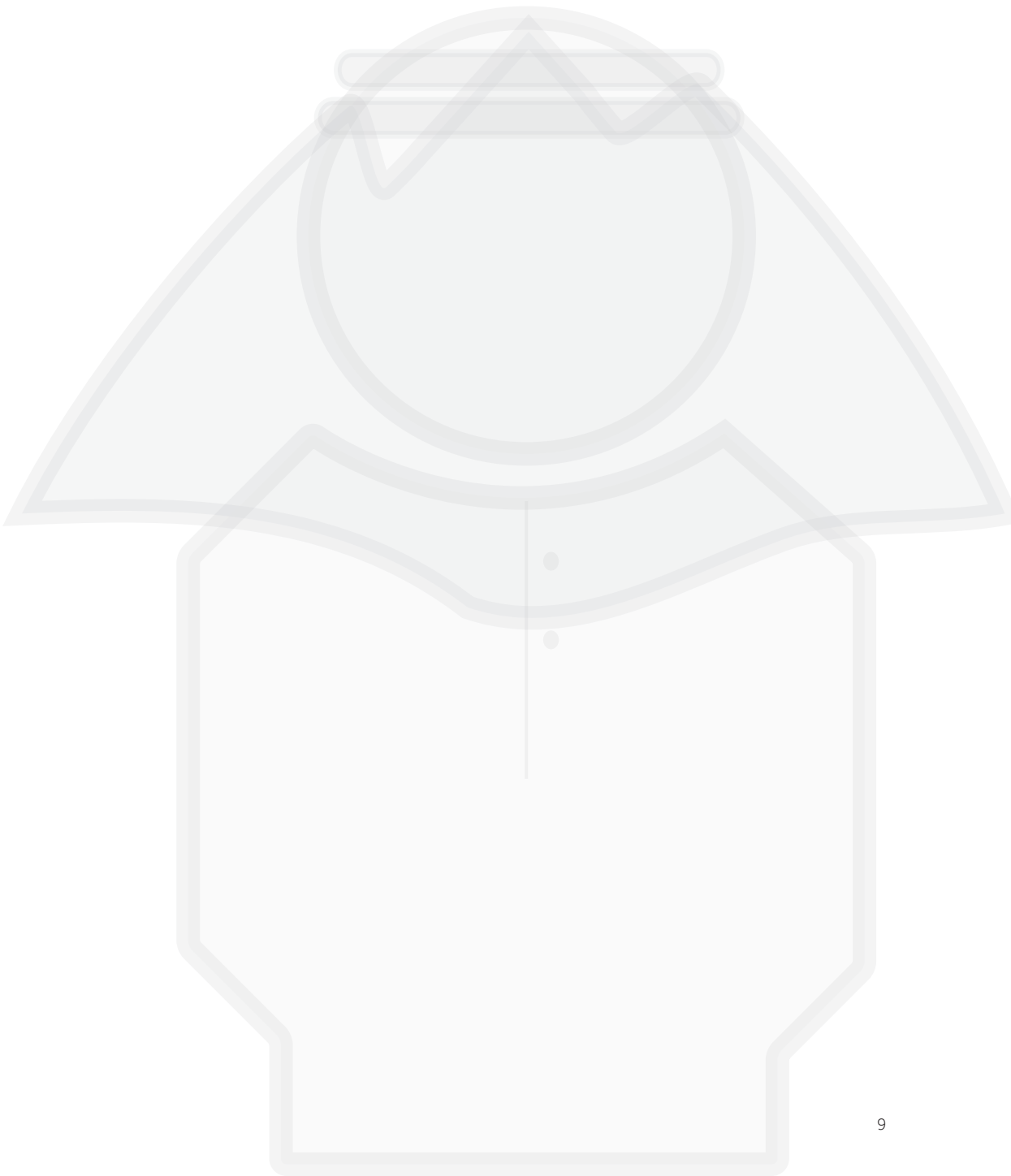
1.2.5 NON-REPUDIATION

Non-repudiation provides the proof of origin of the data. Non-repudiation guarantees that the sender of a message cannot later deny having sent the communication and that the recipient cannot deny having received the communication.

1.3
LIMITATIONS OF EXISTING IA FRAMEWORKS

There are many publicly available Information Assurance (or information security) frameworks, most of which are designed for implementation within a single entity. While many frameworks include provisions for direct network connectivity between certain actors (e.g. purchasing entity and supplier), most do not take into account the IA issues that emerge from the systemic interconnectivity of modern organizations at the sector and national levels.

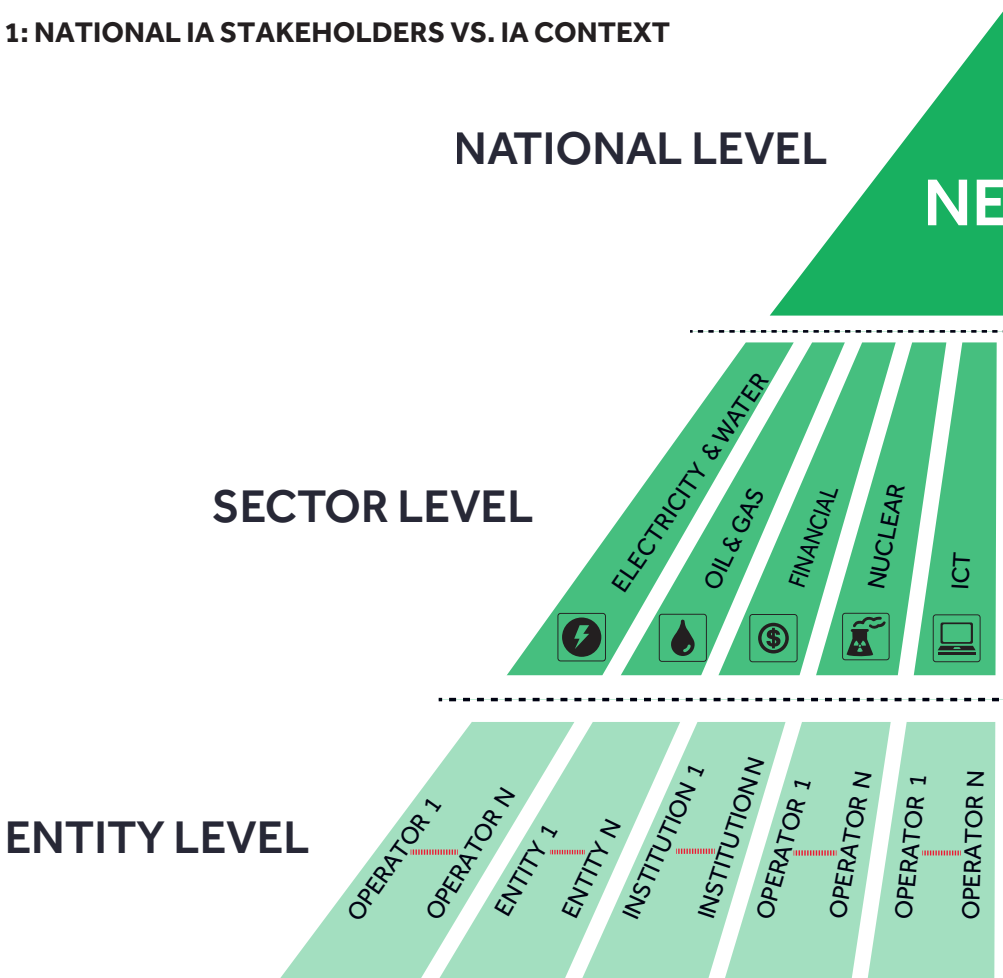
For example, many entities in the UAE have existing IA (or information security) capabilities and internal frameworks. These IA frameworks are based upon a wide range of best practices and have been tailored to meet the needs of each individual entity or specific group of entities, often in a specifically defined context. This approach neither produces comparable results across different entities nor creates a sense of sector or national IA community where all entities across the various sectors work together to address similar IA challenges. This potentially results in overlaps in capabilities that needlessly consume valuable resources and, perhaps more dangerously, could result in security gaps that no single entity or specific group within a sector is able to address in disconnection with others.



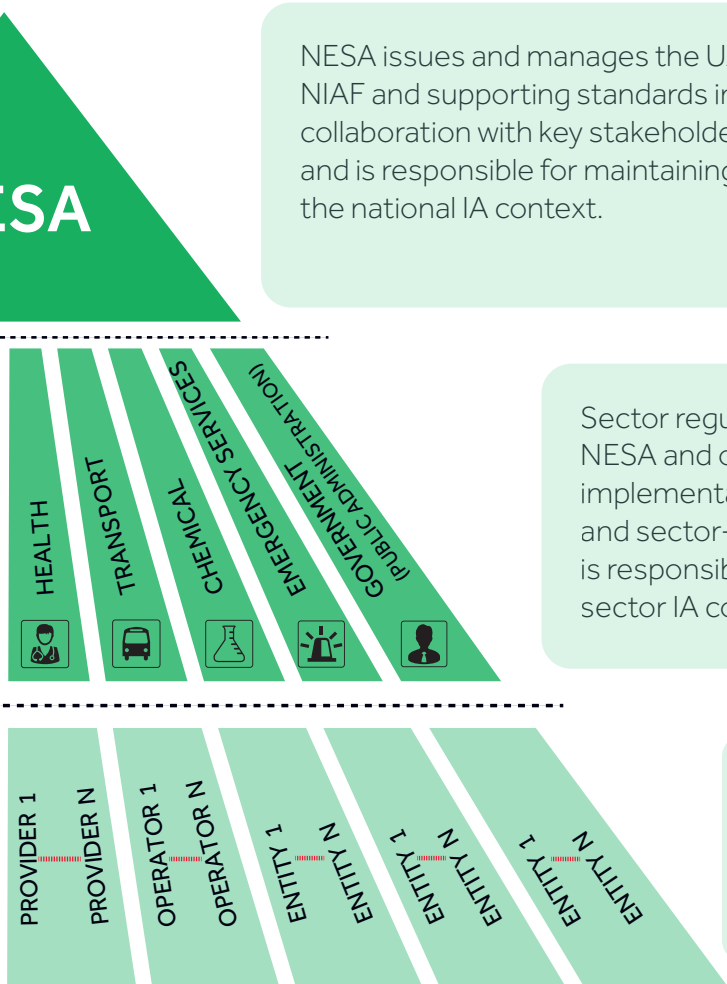
1.4
SECTOR AND NATIONAL IA CONTEXT

To help overcome these limitations the UAE NIAF addresses cybersecurity topics on the entity, sector, and national levels. It outlines a national policy reference that directs and guides the development and implementation of entities' internal IA frameworks and controls.

FIGURE 1: NATIONAL IA STAKEHOLDERS VS. IA CONTEXT



It establishes a minimum IA capability for all UAE entities, while outlining the value-added mechanisms for each entity to integrate into a sector and into national IA context with other stakeholders.



NESA issues and manages the UAE NIAF and supporting standards in collaboration with key stakeholders, and is responsible for maintaining the national IA context.

Sector regulator collaborates with NESA and operators for the implementation of the UAE NIAF and sector-specific standards, and is responsible for maintaining the sector IA context.

Within a sector, entities apply the UAE NIAF and are responsible for maintaining the entity IA context.

Eliminating the silos created by the single-entity approach to IA reduces the risk of gaps, overlaps, and duplicated efforts between individual actors, thereby creating a stronger, integrated national IA context that is better prepared to protect the country from cyber threats.

1.5
APPLICABILITY OF UAE NIAF

Compliance with NIAF will be mandatory for all UAE government entities and other entities identified as critical[1] by NESA in other sectors. For all other UAE entities, NESA highly recommends following the guidelines on a voluntary basis, in order to participate in raising the nation's minimum security levels.

[1]The process for NESA to designate an entity as "critical" is outlined in the UAE Critical Information Infrastructure Protection (CIIP) Policy produced by NESA.

CHAPTER 02

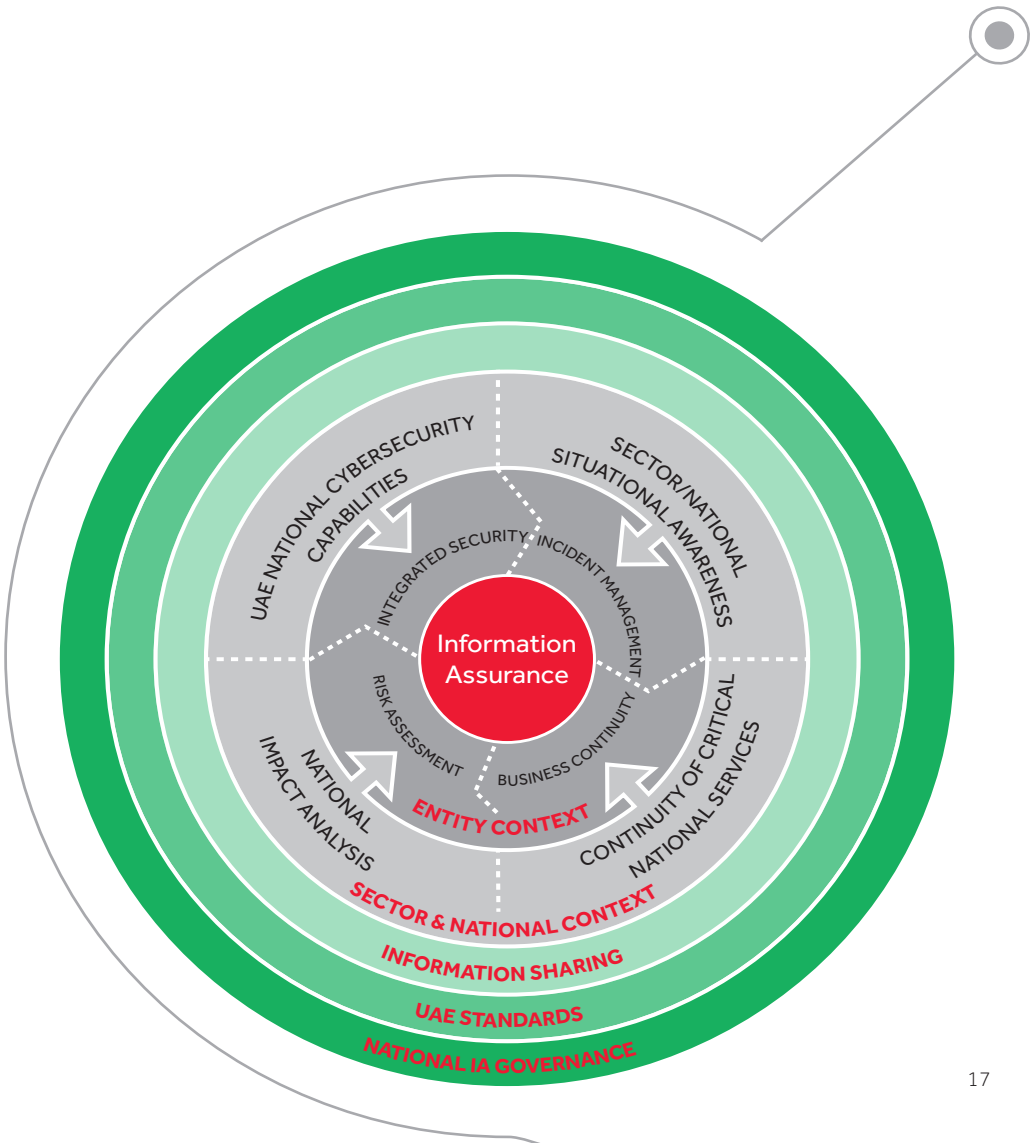
UAE NATIONAL INFORMATION ASSURANCE FRAMEWORK

2.0

UAE NATIONAL INFORMATION ASSURANCE FRAMEWORK

NIAF outlines the entity, sector, and national contexts of IA through a life cycle-based approach supported by a set of UAE standards, effective information-sharing capability and a comprehensive governance program governed by NESA.

FIGURE 2: UAE NATIONAL IA FRAMEWORK



ENTITY CONTEXT

Risk-based approach to identifying and protecting key information assets within an entity.

SECTOR AND NATIONAL CONTEXT

Value-added components that establish the links from an individual entity to the sector and national context.

INFORMATION SHARING

Primary mechanism for entities to effectively exchange information with external actors.

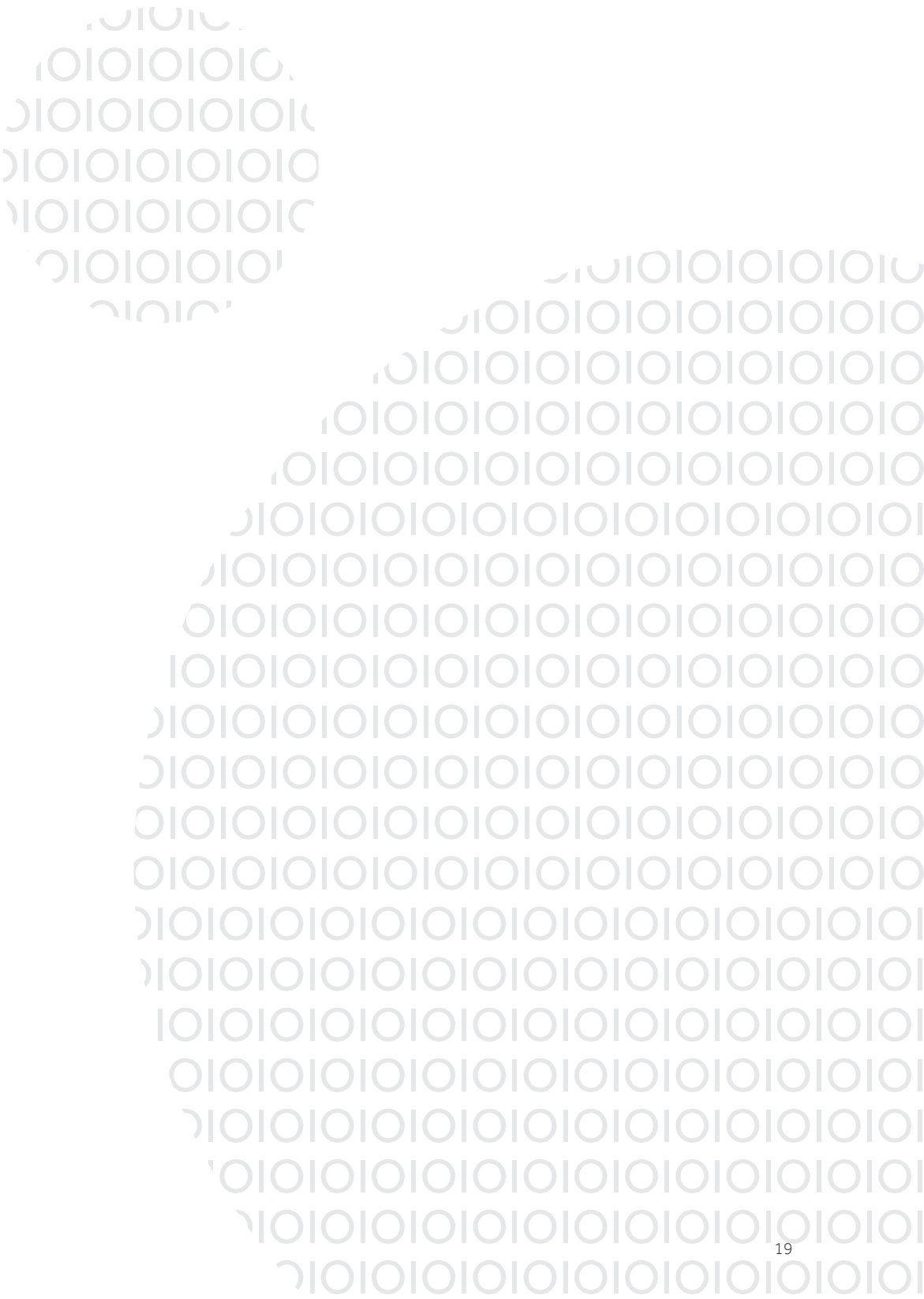
UAE STANDARDS

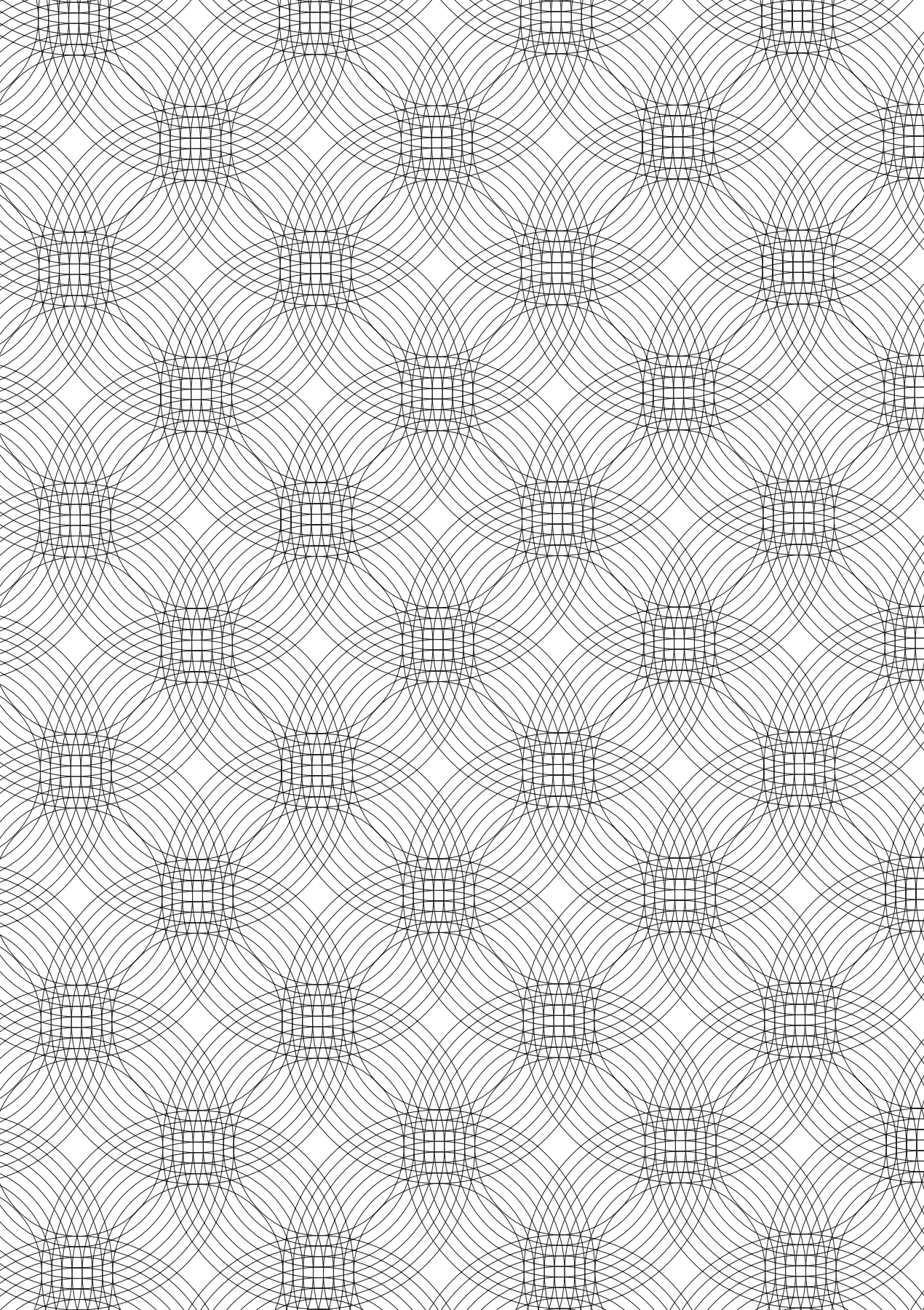
Common, sector-specific and product/service-specific standards applicable to specific entities, sectors, or across all stakeholders.

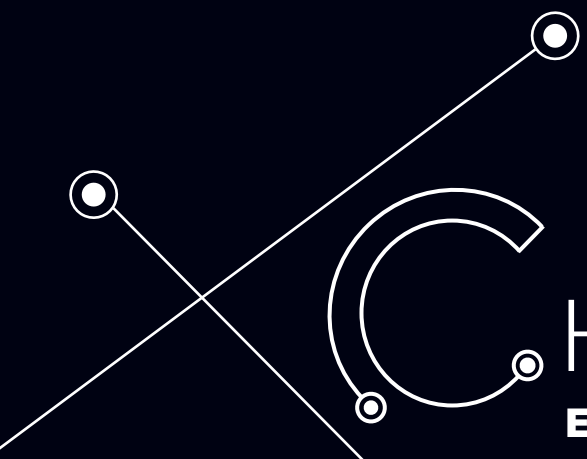
NATIONAL IA GOVERNANCE

Management elements needed to monitor progress and successfully implement the national IA framework.

Through this framework, NESA aims to ensure a minimum level of IA capabilities within all UAE entities and establish a common approach that allows them to interact with each other and approach IA with a sector and national perspective.







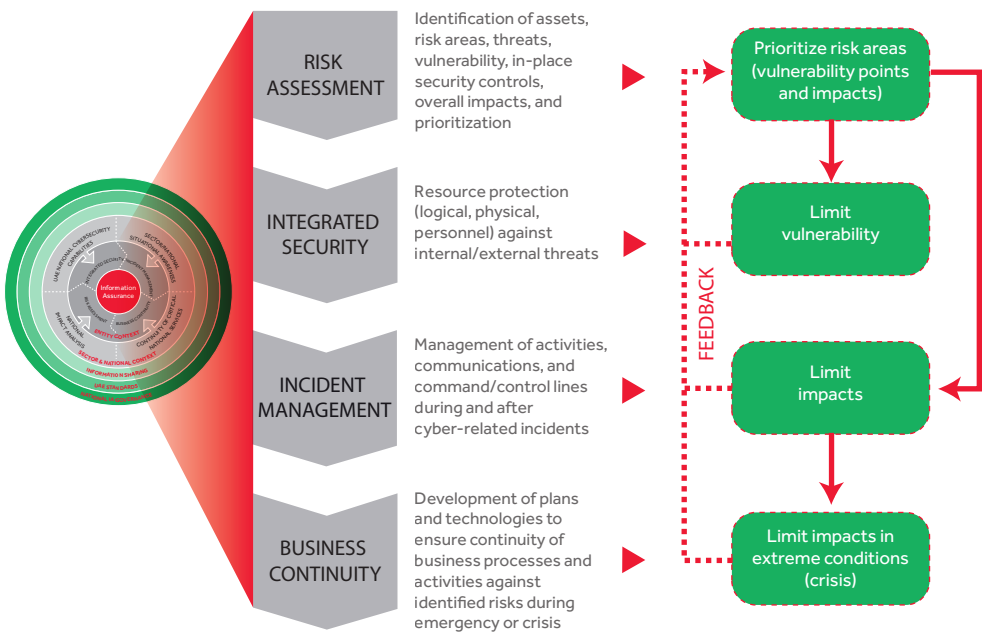
CHAPTER 03

ENTITY CONTEXT

3.0
ENTITY CONTEXT

The IA framework highlights a specific subset of core capabilities necessary to establish a minimum level of IA within each entity, through a life cycle approach. In collaboration with relevant key stakeholders, NESA defines the detailed requirements for each of these capabilities in common, sector-specific, and service/product UAE standards and guidelines.

FIGURE 3: NIAF ENTITY-SPECIFIC CAPABILITIES



3.1
RISK ASSESSMENT

Risk assessment is the central component of an effective life cycle approach to IA, helping to identify the highest risk areas and assisting IA (or information security) managers with the prioritizing and allocation of resources to efficiently reduce overall risk. This requires a systematic and repeatable approach for assessing the posture of cybersecurity systems and networks, enabling expenditures on controls to be balanced against the potential harm of security failures.

The risk assessment methodology outlined here ensures a uniform approach across all entities and produces comparable results, while still offering each entity the freedom needed to leverage its existing processes and meet its own business needs. The National Cyber Security Risk Management Framework provides further detailed description and guidance to critical entities on the appropriate approach and methodology to conduct risk assessment.

3.1.1 ASSET INVENTORY

Each entity must have a clear understanding of the types of information assets (e.g. hardware, software, databases) under its ownership and/or control, for as-is and to-be enterprise architectures.

3.1.2 BUSINESS IMPACT ANALYSIS

Each entity must evaluate the potential impact in case of a security breach or service interruption of its own information assets, including developing a clear understanding of which activities, processes, and functions each individual information asset supports.

3.1.3 VULNERABILITY ASSESSMENT

Each entity must evaluate the threat exposure levels of their key information assets and the likelihood of an assault upon exploiting those vulnerabilities.

3.2
INTEGRATED SECURITY

Based on the results of the risk assessment, the individual entities must document how identified risks will be mitigated. As a minimum, this includes clearly identifying an integrated set of logical, physical, and personnel security controls to be implemented and the underlying rationale for a control selection based on a cost-benefit analysis.

3.2.1 LOGICAL SECURITY

Each entity must define the appropriate logical security controls (e.g. firewalls, encryption, anti-virus, identity management, etc.) required to protect the information assets under its control and or ownership.

3.2.2 PHYSICAL SECURITY

Each entity must define the physical security controls (e.g. door locks, perimeter fence, fire alarms, etc.) required to protect the information assets under its control and or ownership.

3.2.3 PERSONNEL SECURITY

Each entity must define the personnel security controls (e.g. background checks, post-employment return of assets, etc.) required to protect the information assets under its control and or ownership.

3.3
INCIDENT MANAGEMENT

To minimize the impact of cybersecurity incidents, each entity must have the capacity to monitor its own information assets, identify and manage cybersecurity incidents, and escalate incidents to a sector or national level taking into account and utilizing as appropriate the National Incident Management Capability established by NESA.

3.3.1 SITUATIONAL AWARENESS

Each entity must possess the internal capacity to monitor the constant state of its own information assets and an overall awareness of its surrounding environment. This includes the ability to detect internal cybersecurity incidents, and taking into account any threat, warning, or incident-related information received from external sources.

3.3.2 ENTITY INCIDENT RESPONSE

Each entity must develop an internal incident response capability that minimizes the impact of internal incidents or incidents arising from other entities that could affect them directly or indirectly.

The national framework for cybersecurity incident management, as well as other NESA's issuances, define these minimum capabilities to be put in place by the critical entities.

3.3.3 ESCALATION TO SECTOR AND NATIONAL LEVELS

Each entity must have the processes and communication channels in place to escalate a significant incident to the sector level and to the national level, in accordance with the national framework for cybersecurity incident management developed by NESA.

3.4
BUSINESS CONTINUITY

As a result of the business impact analysis, each entity should identify which information assets are the most crucial to the normal functioning of business. Each entity must ensure that these critical business functions will be available to customers, suppliers, and other actors as needed, including during significant cybersecurity events or other incidents (e.g. natural disasters) that might impact availability of these critical information assets. Business continuity is not only implemented at the time of a disaster but requires the performance of daily activities to maintain service, consistency, and recoverability.

3.4.1 CONTINUITY PLANNING

Prior to the occurrence of a disastrous incident, each entity must have developed and regularly tested a plan for continuing critical services and operations under significantly adverse conditions that may impact its critical information assets.

3.4.2 DISASTER RECOVERY

Each entity must have an internal disaster recovery plan that illustrates the process of rapid recovery of critical information assets during a catastrophic interruption.

3.4.3 RETURN TO STEADY STATE

Each entity must define a business resumption plan that ensures the smooth transition of critical information assets back to a state of normal service following a disruption.

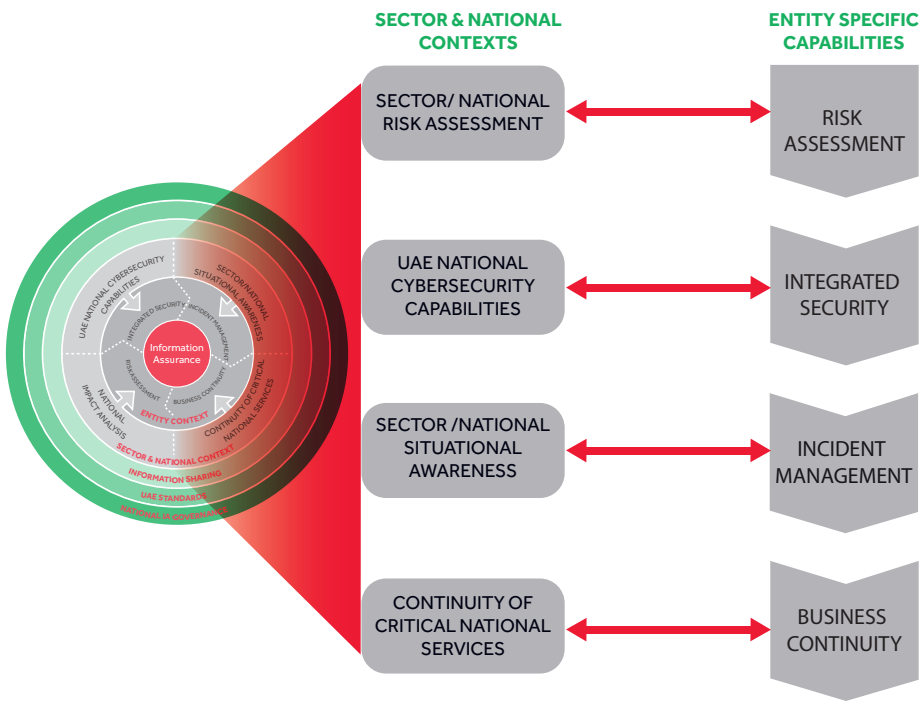
CHAPTER 04

SECTOR AND NATIONAL CONTEXTS

4.0
SECTOR AND NATIONAL CONTEXTS

The outlined entity-specific capabilities are supported by a set of value-added components that help each individual entity extend beyond its own perimeter to connect to the sector and national IA context. These components include:

FIGURE 4: COMPONENTS OF SECTOR/NATIONAL CONTEXT



SECTOR AND NATIONAL RISK ASSESSMENT

Guiding how risk levels from individual entities are integrated to form sector and national views of risk.

UAE NATIONAL CYBERSECURITY CAPABILITIES

Providing entity-level access to national-level cybersecurity capabilities (e.g. developed through research programs).

SECTOR AND NATIONAL SITUATIONAL AWARENESS

Formally sharing predefined types of information within the sector or with other sector(s) and national stakeholders before, during, and after incidents.

CONTINUITY OF CRITICAL NATIONAL SERVICES

Minimizing the downtime of critical national services during crisis-level events.

4.1
SECTOR/NATIONAL RISK ASSESSMENT

The objective of the sector/national risk assessment is to give relevant stakeholders a clear understanding of where the highest levels of systemic risk lie in the UAE and to prioritize the allocation of resources to those areas.

The UAE Critical Information Infrastructure Protection (CIIP) Policy outlines the national risk assessment methodology detailed in the National Risk Management Framework, which ensures that a uniform approach is applied across all entities to produce comparable results, while offering each entity the freedom needed to leverage its existing processes and meet its own business needs. This includes:

- **A methodology[2] for operators to determine which of their information assets support critical national services**
- **Guidance on the types of vulnerabilities to be considered**
- **Indications of the types of threat attributes used to attack specific vulnerabilities**
- **Guidance on the analysis and evaluation of the risk found**
- **A description of how individual entity risk assessment results will be combined to form the sector- and national-level views**

[2]Critical national services are defined in the UAE Critical Information Infrastructure Protection (CIIP) Policy.

4.2
UAE NATIONAL CYBERSECURITY CAPABILITIES

When deemed necessary, NESA will support individual entities in implementing the integrated approach to security by providing access to national-level cybersecurity capabilities, such as:

- **National sharing of capabilities developed within other entities**
- **Specific product prototypes from nationally funded research programs**
- **National security clearances for critical personnel**
- **Advanced network monitoring capabilities**
- **Information on the evolving threat landscape**
- **Access to international stakeholders and capabilities**
- **Other specific topics not generally covered within common national security standards**

Based upon sector and national risk assessment results, NESA will determine where the application of a specific national cybersecurity capability is needed.

4.3

SECTOR AND NATIONAL SITUATIONAL AWARENESS

While managing their own internal incidents, individual entities must also be aware of activities within the environment that surrounds them and adequately share information with other stakeholders before, during, and after significant incidents occur.

NESA will facilitate sector- and national-level awareness by providing a trusted information-sharing capability that allows individual entities to effectively share information on a sector level, and all sectors to share information on the national level. This capability is outlined in the UAE National Information-Sharing Policy.

The national framework for cybersecurity incident management will provide guidance to individual entities on how to evaluate the impact of a breach of confidentiality, integrity, or availability, and how to escalate such a situation to the sector and national level.

4.4

CONTINUITY OF CRITICAL NATIONAL SERVICES

In addition to assuring the continuity of services critical to its own operations, each individual entity is responsible for ensuring the continuity of critical national services that depend on its information infrastructure. In the normal process of business continuity planning within each entity, national requirements must therefore be considered when outlining the parameters used to define backup, short-term and long-term disaster/incident recovery and business resumption capabilities.

NESA, in collaboration with sector regulators and key relevant stakeholders, will provide guidance on the continuity of critical national services, including:

- **Information on calculating the recovery point objective and recovery time objective for critical national services**
- **Disaster recovery requirements for systems supporting critical national services**
- **Reporting requirements for returning critical national services to a stable state**
- **Other relevant guidance support**

CHAPTER 05

INFORMATION SHARING

5.0
INFORMATION SHARING

Information sharing refers to the exchange of information between groups of stakeholders and is critical to effective cybersecurity management capabilities at the national level. Information sharing is the adhesive that binds all national actors together; it is one of the key enablers that differentiates a national IA framework from a stand-alone IA framework. The objective of the UAE NIAF's information-sharing component is to distribute cyber threat information and information security best practices between participating stakeholders to improve their capacity to safeguard information assets.

The National Information-Sharing Policy, as well as other NESA issuances, will detail the requirements for the national information-sharing capability that includes:

PARTICIPATING ENTITIES

Interaction will occur at three layers of interaction; entity, sector, and national. This model provides a manageable information-sharing structure that facilitates the cross-entity and cross-sector exchange of information on cybersecurity topics.

SERVICES PROVIDED

Multiple information-sharing services will be supported by facilities including but not limited to filtered warning, advice brokering, and incident reporting.

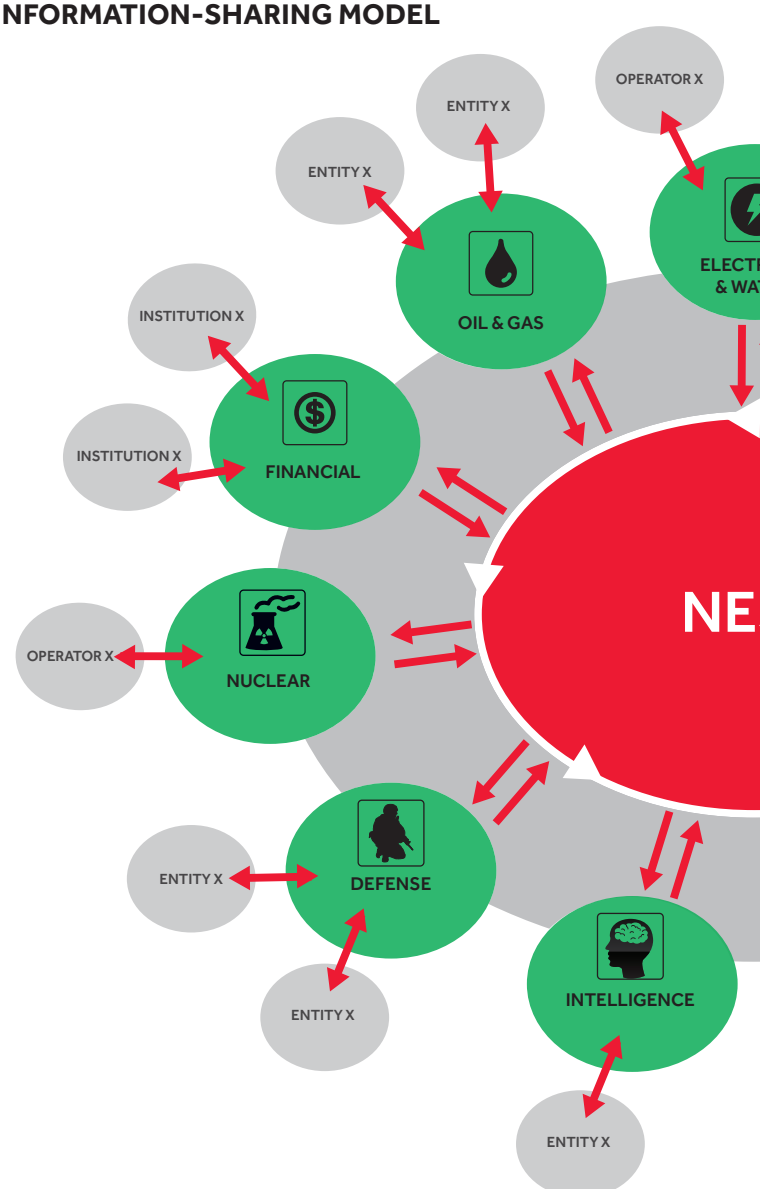
KEY FEATURES

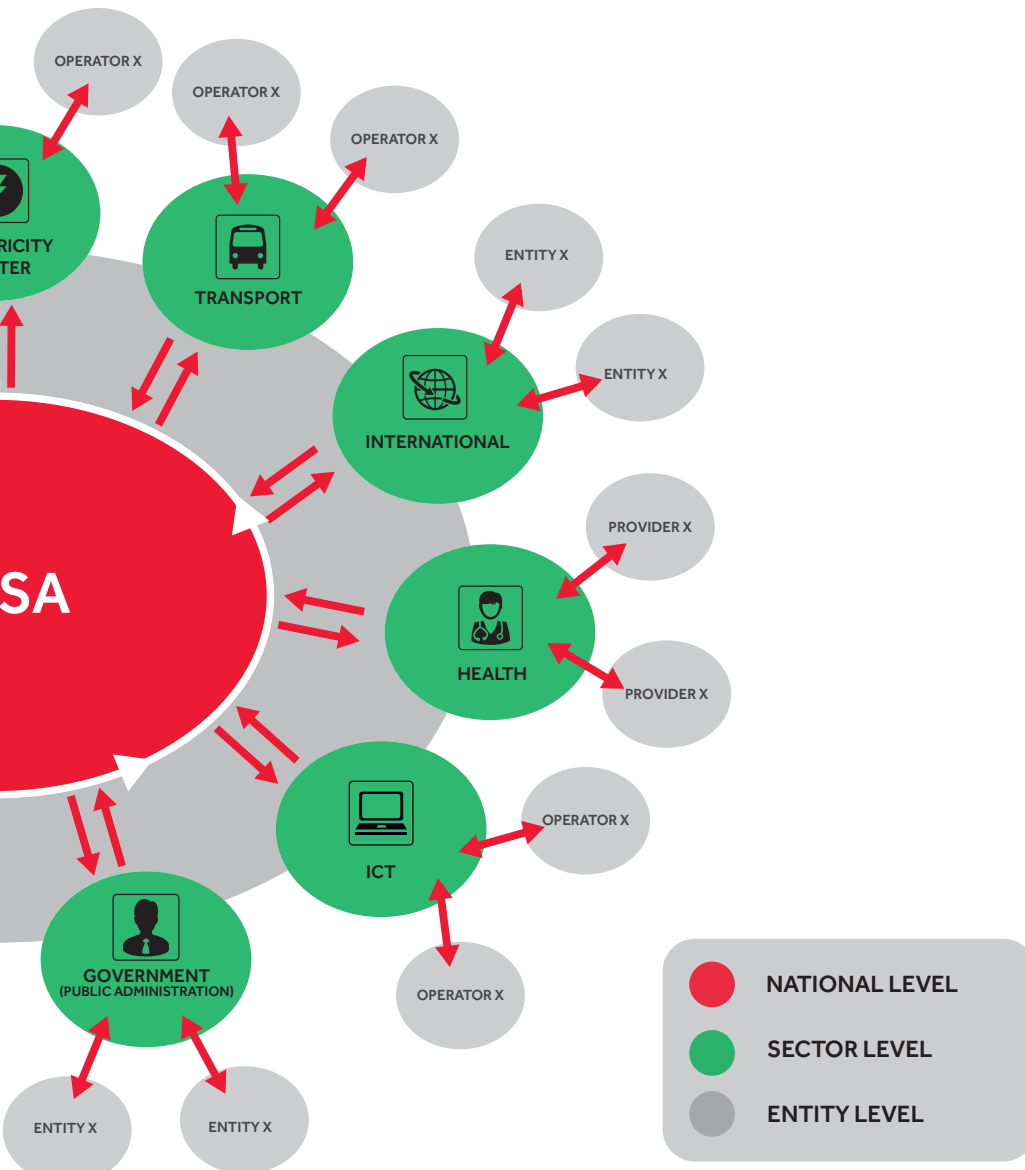
To improve the the information-sharing model, a number of features will be utilized such as secure platform, including anonymity and owner control of information rights.

OPERATING MODEL

This includes delineation of the functional and technical requirements.

FIGURE 5: CONCEPTUAL INFORMATION-SHARING MODEL




OPERATOR X
OPERATOR X
OPERATOR X
TRANSPORT
ENTITY X
ENTITY X
INTERNATIONAL
PROVIDER X
HEALTH
PROVIDER X
OPERATOR X
ICT
OPERATOR X
GOVERNMENT
(PUBLIC ADMINISTRATION)
ENTITY X
ENTITY X
NATIONAL LEVEL
SECTOR LEVEL
ENTITY LEVEL

CHAPTER 06

UAE STANDARDS

6.0
UAE STANDARDS

UAE Standards raise the IA capabilities within all entities to a common minimum required level and to establish the components required to unite these actors within a sector and national context.

The three levels of UAE IA Standards are:

- **Common Standards that is applicable to all entities across different sectors**
- **Sector-specific Standards that address aspects specific to the characteristics of individual sectors**
- **Service and Product-specific Standards that are tailored to the needs of specific services and products**

NESA, in collaboration with sector regulators and key stakeholders, will review these standards periodically, or as needed, and validate their continued relevance.

6.1
COMMON STANDARDS

Common Standards define a minimum level of IA capabilities and cybersecurity controls that every entity in the UAE must strive to meet; compliance with these standards is mandatory on specific cases and identified stakeholders. The Standards outline the general management and technical requirements that are to be applied, irrespective of the sector or activity the entity is engaged in.

All UAE government and other entities identified as critical[3] by NESA in other sectors must demonstrate compliance with the Common Standards, although certification by these standards may not be required.

[3]The process for NESA to designate an entity as "critical" is outlined in the UAE CIIP Policy.

6.2
SECTOR-SPECIFIC STANDARDS

Every sector has unique characteristics and operational complexities that may not apply to other sectors. As a result, the types of cybersecurity threats and vulnerabilities entities must manage in their specific sectors can vary greatly. For example, Industrial Control Systems (ICS) used in the electricity sector present cybersecurity challenges that are not relevant for the financial sector.

To address these sector-specific challenges, NESA will develop sector-specific standards as needed in consultation with sector regulators, respective ministries, technical authorities, as well as the sector entities/operators. In specific cases, sector regulators in coordination with NESA may also decide to issue further technical guidelines to help entities implement their Sector-specific Standards.

Each Sector-specific Standard will outline how NESA, respective regulators and sector-specific entities will collaborate to implement such measures.

6.3
SERVICE AND PRODUCT-SPECIFIC STANDARDS

When required, NESA will develop tailored standards for specific services and products. Based upon interaction with relevant stakeholders, NESA will determine when a service or product-specific standard is needed, and the type and level of security controls required. Given the ad-hoc nature of these types of standards, the scope and applicability of each will be defined within the standard itself.

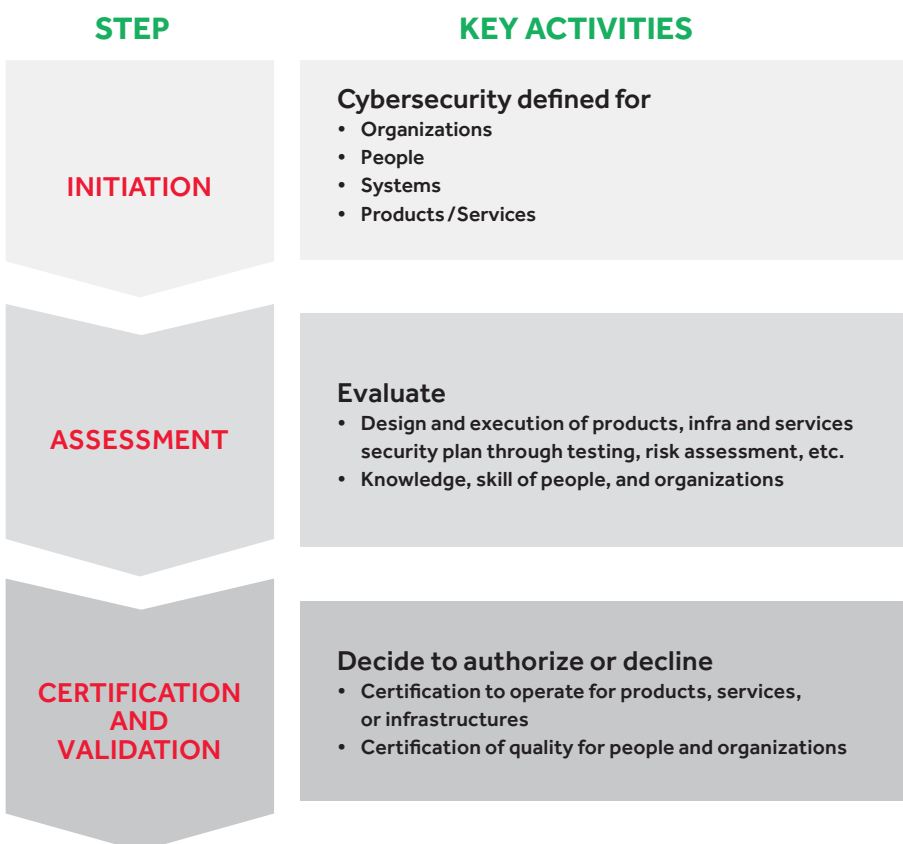
6.4
CERTIFICATION

In certain cases to be defined by NESA, stringent verification of compliance with a specific national standard may be required. The Framework for Compliance, Certification, and Accreditation outlines how NESA validates and classifies levels of compliance against implementation and/or quality requirements defined in the UAE IA Standards.

This certification program covers the UAE Standards applicable to persons, organizations, systems, services, and products.

The certification process consists of three steps:

FIGURE 6: CERTIFICATION PROCESS



The UAE Certification Against UAE IA Standards Policy outlines the detailed activities along each step of the certification process.

6.5
INFORMATION ASSURANCE TECHNICAL FORUMS

The Information Assurance Technical Forums (IATF) organized by NESA provide an avenue for relevant stakeholders to share their experiences and lessons learned in implementing the UAE IA Standards. During the Forums, stakeholders can also seek clarifications or raise their standard implementation concerns or challenges.

Members of the IATF would include industry leaders, vendors, academia, government agencies, and technical experts for general review and discussion of the IA Standards at various levels.

The Forums aim to foster stakeholders' engagement and experience/information-sharing in a wide range of technical topics to increase the level of awareness and knowledge on cybersecurity and related best practices.

CHAPTER 07

NATIONAL IA GOVERNANCE

7.0
NATIONAL IA GOVERNANCE

The UAE NIAF Governance Model defines how NESA will interact with stakeholders and monitor compliance with the NIAF, including the:

- **Method NESA will use to interact with stakeholders on the implementation of NIAF**
- **Impact of organizations' implementation of NIAF overall (e.g. required Liaison Officers (focal coordinators) in stakeholder organization)**
- **Expectations regarding the requirements for stakeholders reporting to NESA**
- **Tools at NESA's disposal to promote and ensure compliance**

7.1
STAKEHOLDER INTERACTION WITH NESA

To effectively manage NIAF implementation, NESA should communicate and coordinate with a wide range of relevant key entities. To facilitate these activities, each of these entities should then designate at least one named individual as its Liaison Officer (focal coordinator), responsible for coordinating issues with NESA and other government agencies. The entities will communicate the name and contact details of their Liaison Officer to NESA.

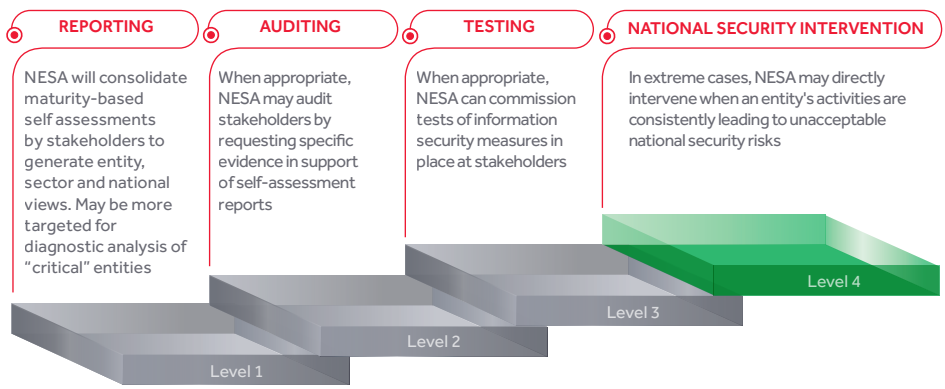
The UAE NIAF Governance Model defines the requirements for an individual to be named as the Liaison Officer within each entity.

In cases where the entity intends to replace or temporary substitute its Liaison Office, NESA shall be informed by the entity before such action is taken.

7.2
COMPLIANCE MONITORING

The figure below describes the four levels of monitoring that NESA will use to manage stakeholder compliance across all aspects of NIAF:

FIGURE 7: ESCALATION OF COMPLIANCE MONITORING SCHEMES



The UAE NIAF Governance Model will provide further details of the process under which NESA may choose to elevate the level of compliance monitoring within a specific entity or sector.

ANNEXES

ANNEX 1

NIAF SUPPORTING INSTRUMENTS

NIAF Component	Supporting Instruments
Entity Context	• To be defined
Sector/National Context	• UAE National Risk Management Framework • UAE National Cyber Response Framework • UAE Critical Information Infrastructure Protection Policy
Information Sharing	• National Cybersecurity Information-Sharing Policy
National Standards	• UAE Information Assurance Standards • National Framework for Compliance, Certification, and Accreditation
National IA Governance	• UAE NIAF Governance Model

ANNEX 2

KEY DEFINITIONS

TERM	DEFINITION
CRITICAL SERVICE [4]	Vital service, the disruption or destruction of which may have a debilitating impact on the national security, economy, society, or any combination of these.
CYBERSECURITY	Is the set of capabilities (including processes, practices, and technologies) designed to protect the cyber (including information) assets from being penetrated, compromised, or disrupted.
CYBERSPACE	The domain within the information environment consisting of the interdependent network of information and communication technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers[5].
ENTITY CONTEXT	Refers to the set of entity information assets, practices, and standards that characterize core cybersecurity capabilities to establish a minimum level of Information Assurance within a given entity.
INFORMATION ASSET	A physical or virtual asset of ICT systems such as data, systems, facilities, networks, and computers.
INFORMATION ASSURANCE	Practice of protecting information and managing risks and continuity related to the use, processing, storage, and transmission of information or data, and the systems and processes used for those purposes. The Information Assurance is a superset of information security; it covers a much broader range of information protection and management aspects including business/information continuity, disaster recovery, compliance, certification, and accreditation, etc.

UAE COMMON INFORMATION ASSURANCE STANDARD	Custom UAE Standard that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).
NATIONAL CONTEXT	Refers to the set of national information assets, practices, and standards that characterize core cybersecurity capabilities to establish a minimum level of Information Assurance at a national level.
OPERATOR	An entity operating in a particular sector (or market).
REGULATOR	A government body that sets regulations and monitors compliance and behavior of regulated entities in a particular sector (or market).

[4] Detailed criteria used to define a critical service will be outlined in phase one of the UAE CIIP process.
[5] Very similar to the definition by the U.S. Department Of Defence (DOD)

ANNEX 3

ACRONYMS

CIIP	CRITICAL INFORMATION INFRASTRUCTURE PROTECTION
IA	INFORMATION ASSURANCE
IATF	INFORMATION ASSURANCE TECHNICAL FORUMS
ICS	INDUSTRIAL CONTROL SYSTEMS
ICT	INFORMATION AND COMMUNICATION TECHNOLOGIES
ISMS	INFORMATION SECURITY MANAGEMENT SYSTEM
NESA	NATIONAL ELECTRONIC SECURITY AUTHORITY
NCSS	NATIONAL CYBER SECURITY STRATEGY
NIAF	NATIONAL INFORMATION ASSURANCE FRAMEWORK