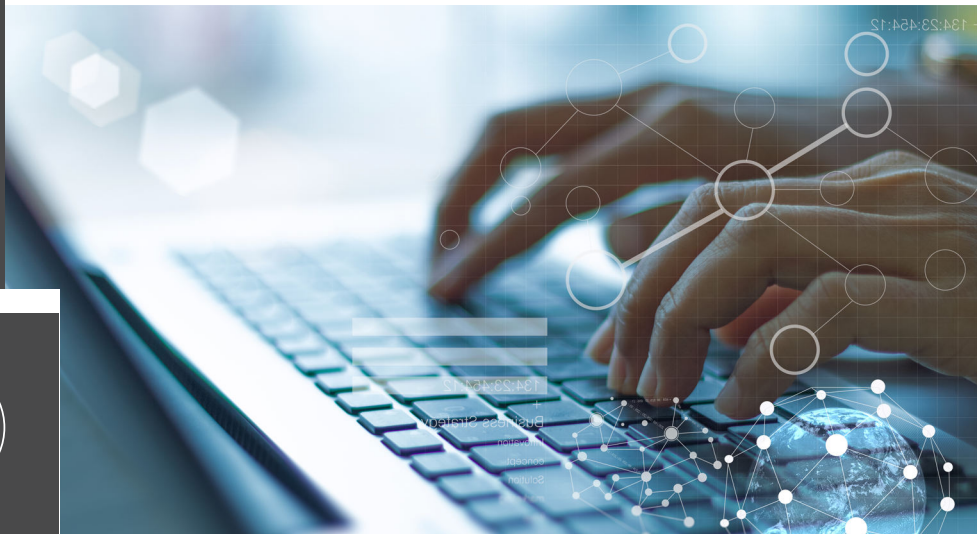
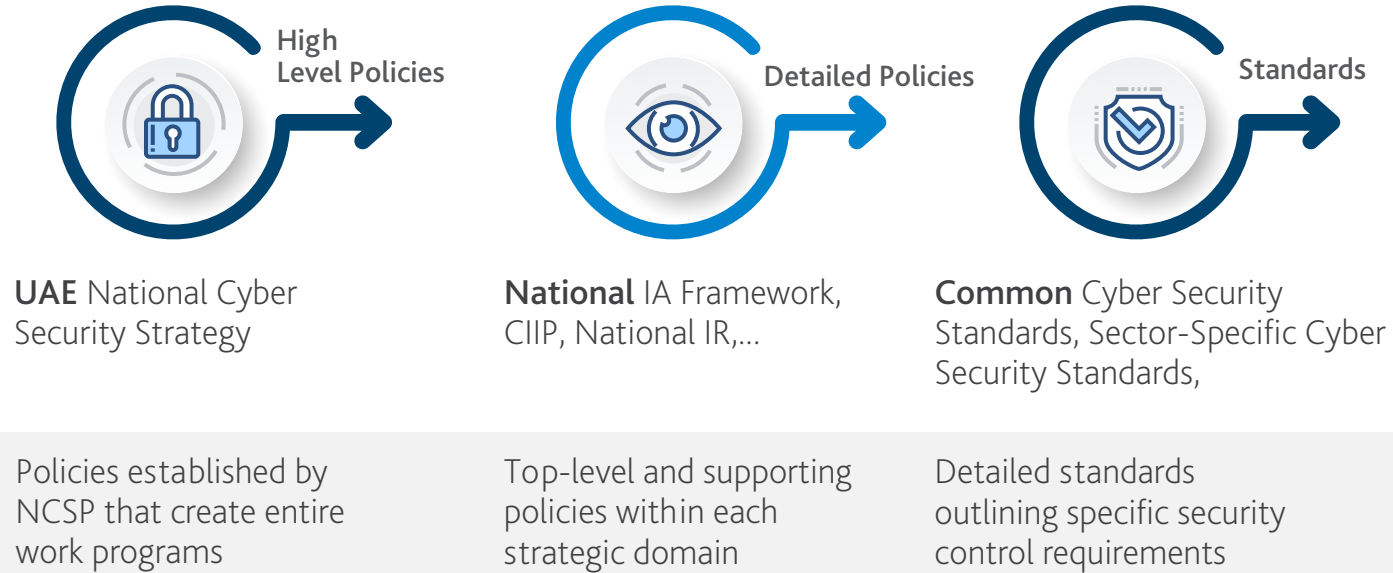


National Security Strategy



Structure of National Cyber Security Plan (NCSP)





Main National Cyber Security Policies

The telecommunication regulatory authority has issued a number of important policies and standards to identify national trends in the field of cyber security and to unify efforts in this regard



THE NATIONAL CYBER
SECURITY STRATEGY



THE NATIONAL INFORMATION
ASSURANCE FRAMEWORK



CRITICAL INFORMATION
INFRASTRUCTURE
PROTECTION POLICY



NATIONAL INFORMATION
ASSURANCE STANDARDS

Cyber Security Strategy Framework



The National Strategy aims at To establish a path to achieve the national vision to secure state information and advice.

In order to do so, this national strategy is designed from five core areas:



The national cyber security strategy aims to chart a path to achieve the national vision to secure national information and communications. In order to do so, this national strategy has been designed from five core areas:

| Strategic Focus Areas | | Definition | Main Objectives | |
|-----------------------------|--|------------|---|--|
| Prepare and Prevent | Strengthen the security of UAE cyber assets and reduce corresponding risk levels | ▶ | Elevate the Minimum Protection Level of Cyber Assets | Ensure Compliance to UAE Cyber Security Standards and Verify Effectiveness |
| Respond and Recover | Manage incidents to reduce impact on society and the economy | ▶ | Develop and Embed Incident Response Management Capabilities | Improve Threat Neutralization Capabilities |
| Build National Capability | Cultivate cyber security research and innovation and develop UAE's workforce to meet cyber security needs | ▶ | Inform and Educate UAE Public and Workforce | Foster Cyber Security Research and Innovation |
| Foster Collaboration | Foster collaboration between national and international stakeholders to catalyze cyber security efforts | ▶ | Cultivate a Collaborative National Cyber Society | Leverage and Contribute to International Efforts |
| Provide National Leadership | Provide national leadership to orchestrate local and emirates cyber security initiatives at the national level | ▶ | Develop National Cyber Security Strategy and Implementation Initiatives | Coordinate and Guide National Cyber Security Implementation |

Principles of Successful NCSS Implementation

Integrated Planning



The importance of the involvement of all key stakeholders in the integrated planning process to ensure:

- Permanent cooperation and joint activities among all stakeholders
- Identify existing challenges and ways to overcome them
- Disseminate relevant information to reach the competent authorities in a timely manner
- Reduce gaps and overlap between different initiatives and activities.

Shared Operational Responsibilities



To ensure effective implementation, it is essential that the various entities involved at the operational level and participate in various cyber security initiatives and activities.

Monitored Progress and Improvement



- Follow up the implementation stages and the effectiveness of the results to ensure appropriate improvements and overall success of the program.
- Ensure effective performance management, support and guidance.

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

Framework



UAE National IA Framework

| | | |
|---|-----------------------------|--|
| 1 | Entity Context | Risk-based approach to identifying and protecting key information assets within an entity |
| 2 | Sector and National Context | Value-added components that establish the links from an individual entity to the sector and national context |
| 3 | Information Sharing | Primary mechanism for entities to effectively exchange information with external actors |
| 4 | UAE Standards | Common, sector-specific and product/service-specific standards applicable to specific or across all stakeholders |
| 5 | National IA Governance | Management elements needed to monitor progress and successfully implement the national IA framework |

Through this framework, TRA 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.

National Level

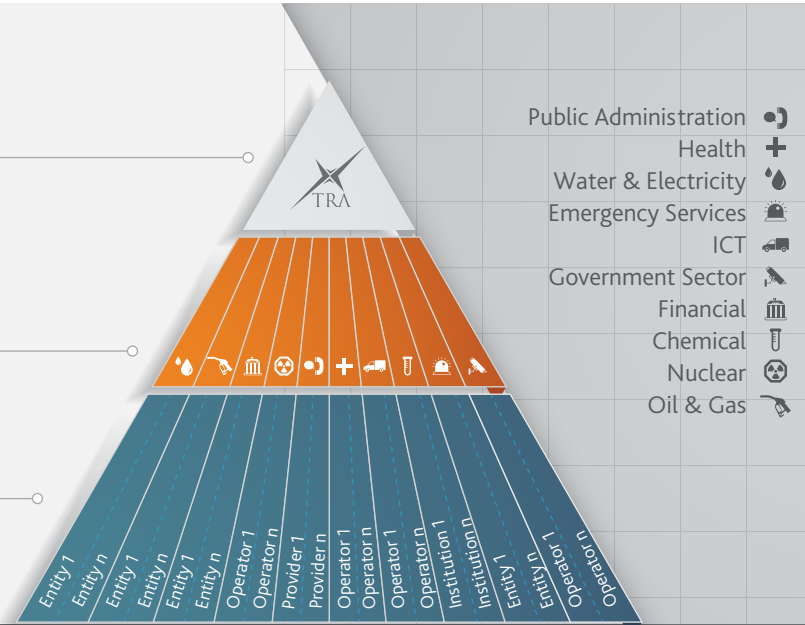
NCSA issues and manages the UAE NIAF and supporting standards, and is responsible for maintaining the national IA context

Sector Level

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

Entity Level

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



The purpose of this policy is to identify and develop the necessary application programs to protect Critical information infrastructure:






Policy



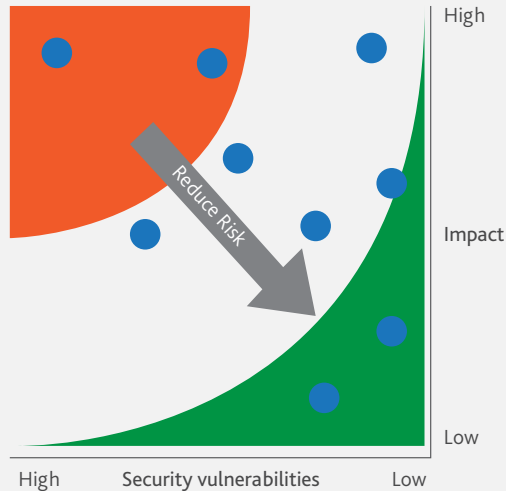
Protection of Critical Information Infrastructure

- 1 Identification of programs for the protection of Critical information infrastructure
- 2 Develop a general national approach to identify critical information infrastructures
- 3 Identification of electronic security requirements for Critical information infrastructures and compliance areas
- 4 Defining the main roles and tasks of the main stakeholders
- 5 Develop a general approach to enhance cooperation and communication between Critical sectors

The policy also sets out the key stages of applying risk reduction to critical information infrastructures

-  Financial sector
-  Transportation
-  Electricity and water
-  Oil and gas
-  Critical information infrastructure

Reducing risks in vital sectors



Stages of risk reduction

Conduct Sector Baseline

- Prioritization of Sectors for Implementation
- Engagement of Stakeholders
- Identification of Critical National Services

Perform Sector/ National Risk Assessment

- Identification of Supporting Critical Information Infrastructure
- Threat and Vulnerability Assessment
- Sector and National Cybersecurity Risk Assessment

Define Sector Plans

- Identification of CII Cybersecurity Requirements
- Definition of Sector Plans

Monitor Implementation of Sector Plans

- Implementation of Sector Plans
- Monitoring of Implementation



National standards for information security protection
General standards

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

The Common Standard



The Information Assurance Standards

| | | |
|---|---|---|
| 1 | Increase level of protection | Provide minimum requirements to increase the level of protection of information systems and supporting systems |
| 2 | Prioritization of controls | Applying the standards by a methodology that takes into consideration potential risks |
| 3 | Defining roles and responsibilities | Applying the standards by a methodology that takes into consideration potential risks |
| 4 | Standards applicability to other criteria | Complements the information security standards currently in place in the relevant authorities |
| 5 | Source of unified national standards: | Providing unified national standards to ensure the security of information in all concerned entities in the country |

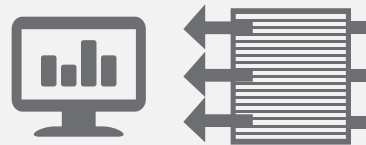
Standards development stages

Several leading international standards in information security have been analyzed and studied as a key reference to the development of The Information Assurance Standards

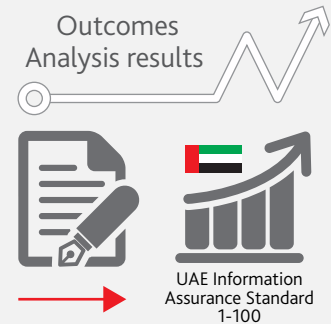
Leading standards for Information assurance standards



Axes of analysis

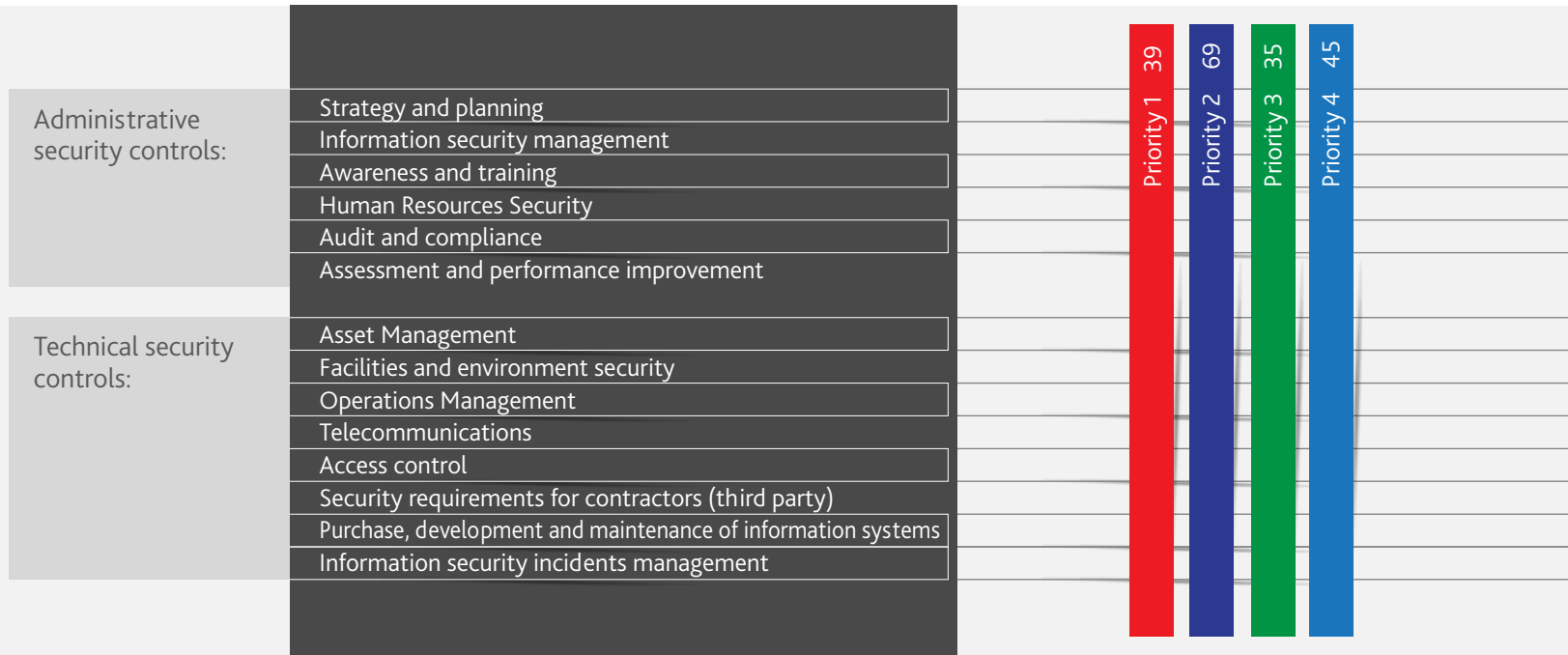


- Scope of controls
- Controls details
- How easy to use
- Prioritization of controls
- Implementation results and global recognition



The standards for the UAE have been developed, To include the most important areas of other standards

The standards consist of two main sets of security controls (administrative and technical), there are 188 controls distributed over 15 main areas and prioritized according to four priorities.



The entities will participate in the implementation of the INFORMATION ASSURANCE STANDARDS and the development of sector standards in accordance with the Critical information infrastructure protection policy through communication and cooperation with the relevant critical entities

Summary of roles:

