

Do you have a specific NIAF version or publication year to include? If not, should I use the generic banner



What it is

The UAE National Information Assurance Framework (NIAF) is a national cybersecurity and information assurance framework that helps organizations in the United Arab Emirates safeguard critical information assets and strengthen their security posture. The framework establishes minimum requirements for protecting government, semi-government, and regulated entities against evolving cyber threats and ensuring compliance with national data protection objectives.

The NIAF is published by the United Arab Emirates Telecommunications and Digital Government Regulatory Authority (TDRA) and is required for federal and select industry organizations that manage sensitive or critical infrastructure. It covers a broad set of areas including cybersecurity controls, risk management, privacy governance, and incident response, aligning with international standards while addressing UAE-specific regulatory requirements.

At a glance

<div>PUBLISHER</div> <div>Telecommunications and Digital Government Regulatory Authority (TDRA)</div>	<div>TYPE</div> <div>Framework</div>	<div>VERSION</div> <div>2020</div>
<div>DOMAIN</div> <div>Cybersecurity</div>	<div>FAMILY</div> <div>Other</div>	<div>REGION</div> <div>United Arab Emirates</div>
<div>ADOPTION MODEL</div> <div>Regulatory Compliance</div>	<div>IMPLEMENTATION COMPLEXITY</div> <div>High</div>	

Source: <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/-/media/Documents-2023/National-Information-Assurance-Framework-NIAF.ashx>

Why it matters

- **Strengthen information assurance governance** Enable organizations to systematically identify, manage, and mitigate cybersecurity risks in alignment with national priorities.
- **Enhance regulatory compliance** Support adherence to UAE laws and regulations, reducing legal exposure and safeguarding organizational reputation.
- **Increase audit readiness** Provide structured guidance for documenting, monitoring, and reporting security controls, facilitating efficient internal and external audits.
- **Promote operational resilience** Help organizations maintain continuity of essential services by reducing vulnerabilities and improving incident response capabilities.

How SmartSuite supports UAE NIAF

National Control Framework Library

Structure NIAF control domains with ownership, scope, and implementation tracking.

NIAF Risk and Control Mapping

Link organizational risks to NIAF controls and manage mitigation activities.

Policy, Standards, and Governance Management

Centralize security policies, standards, and approvals aligned to UAE requirements.

Access Control and Security Operations

Manage identity, authentication, and operational security controls across systems.

Monitoring, Incident Response, and Continuity

Track security events, manage incidents, and ensure operational resilience.

Compliance Monitoring and Audit Reporting

Provide dashboards showing control coverage, risk posture, and NIAF compliance readiness.

Common framework mappings

- CIS Controls v8.1
- COBIT 2019
- GDPR
- ISO 27001:2022
- NIST CSF 2.0
- NIST 800-53 Rev.5
- PCI DSS 4.0.1
- SOC 2

Official resources

Frequently asked questions

What is the UAE NIAF used for?

The UAE NIAF is designed to establish baseline requirements and best practices for information security within public and private sector organizations operating in the UAE. Its purpose is to enhance national cybersecurity by ensuring critical information assets are protected against threats and vulnerabilities.

Is compliance with UAE NIAF mandatory?

Compliance with UAE NIAF is mandatory for all government entities and certain designated critical infrastructure organizations in the UAE. While not all private sector organizations are required to follow NIAF, adherence is strongly encouraged for improved risk management and regulatory alignment.

Who does the UAE NIAF apply to?

The UAE NIAF applies to government bodies and organizations operating critical national infrastructure within the UAE. It may also be adopted by private sector organizations looking to align with national cybersecurity policies or subject to specific regulatory directives.

What are the key requirements or control areas in UAE NIAF?

UAE NIAF covers control areas such as information asset management, risk assessment, incident response, access control, information security policy, and ongoing monitoring. Organizations are required to document policies, risk assessments, technical and organizational controls, and maintain logs evidencing compliance.

How should organizations implement the UAE NIAF controls?

Implementation typically begins with a gap assessment against NIAF requirements, setting the scope, and developing policies and procedures that address the framework's controls. This includes assigning accountability, conducting risk assessments, and establishing mechanisms for continuous improvement and monitoring.

How does the UAE NIAF relate to other standards like ISO 27001?

UAE NIAF aligns closely with international standards such as ISO 27001, but it is specifically tailored to meet the legal, regulatory, and threat landscape within the UAE. Organizations already compliant with ISO 27001 will find significant overlap, but must address unique UAE-specific obligations in NIAF.

What are the ongoing compliance requirements for UAE NIAF?

Organizations must regularly review and update their security policies, perform risk assessments, conduct training and awareness sessions, and monitor control effectiveness. Periodic internal audits and compliance reporting are necessary to demonstrate adherence to NIAF requirements.

How would SmartSuite support UAE NIAF?

SmartSuite can support UAE NIAF compliance by providing tools for risk tracking, control management, and centralized evidence collection. The platform helps streamline audit readiness with task assignment, automated reminders, and comprehensive reporting features, making it easier to maintain and demonstrate continuous compliance with the framework.

License included / downloadable: Yes The UAE National Information Assurance Framework is published by the UAE National Electronic Security Authority (NESA) and is publicly available for download from official UAE government/NESA websites. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/uae-niaf-national-information-assurance-framework