SmartSuite

Framework / Cybersecurity / Other

UAE National Information Assurance Framework (NIAF)

The UAE National Information Assurance Framework (NIAF), issued by NESA, sets entity, sector and national information assurance requirements for UAE government and critical entities.



What it is

The UAE National Information Assurance Framework (NIAF) is the national policy framework that sets out how information assurance is achieved at the entity, sector and national levels in the United Arab Emirates. It was issued by the National Electronic Security Authority (NESA), and under section 1.5 compliance is mandatory for all UAE government entities and for other entities that NESA identifies as critical under the Critical Information Infrastructure Protection (CIIP) Policy; other UAE entities are urged to follow it voluntarily.

At a glance

PUBLISHER National Electronic Security Authority (NESA) for the NIAF; Telecommunications and Digital Government Regulatory Authority (TDRA) for IA Regulation v1.1	TYPE Framework	VERSION NIAF with UAE Information Assurance Regulation v1.1
EFFECTIVE Mandatory for UAE government and designated critical entities; no commencement date is stated in the documents	DOMAIN Cybersecurity	FAMILY Other
REGION United Arab Emirates	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: u.ae/en/information-and-services/justice-safety-and-the-law/Safety/cyber-safety-and-digital-security

Why it matters

- **A national baseline** Compliance is mandatory for all UAE government entities and entities identified as critical (section 1.5), which sets the minimum for the sectors in the CIIP Policy.
- **Entity, sector and national views** Entity results roll up through sector regulators to the national level, so each entity's report feeds a national picture of risk.
- **Five assurance principles** Confidentiality, integrity, availability, authentication and non-repudiation (section 1.2) define what information assurance must deliver.
- **Risk-based control selection** The IA Regulation lets an entity exclude a control only with a justification submitted to the regulator, except for the Always Applicable controls.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports UAE NIAF

Entity Context Register

Keep the asset inventory, business impact analysis and vulnerability assessments required by section 3.1 with owners and review dates.

IA Regulation Control Library

Load management families M1 to M6 and technical families T1 to T9 with priority level, Always Applicable status and implementation state.

Applicability and Exclusions

Record each control excluded after the risk assessment with its justification and the risk acceptance by the accountable person.

Incident Escalation and Continuity

Track incidents with their escalation to sector and national levels, and link critical services, business impact analysis records and recovery plans in Operational Resilience & Business Continuity.

Regulator Reporting

Assemble self-assessment reports, audit evidence and test results for the sector regulator, and record the Liaison Officer and reporting dates.

Third Party Security

Track contractors and service providers against the third-party family T6 with Third Party Risk Management, including due diligence and review dates.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | 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 National Information Assurance Framework and who issued it?

The NIAF is the national framework for information assurance in the UAE, issued by the National Electronic Security Authority (NESA) to support the UAE National Cyber Security Strategy. It sets out how entities, sectors and the national level share responsibility for information assurance. It names the controls only by reference to the UAE Information Assurance Standards, which are separate documents.

Who must comply with the NIAF?

Section 1.5 makes compliance mandatory for all UAE government entities and for other entities that NESA identifies as critical, under the process in the CIIP Policy. For all other UAE entities the framework is recommended on a voluntary basis. The IA Regulation adds that the regulator designates the critical entities that must implement it.

What are the entity, sector and national contexts?

The entity context (chapter 3) is the four capabilities each entity builds: risk assessment, integrated security, incident management and business continuity. The sector and national contexts (chapter 4) connect entities through sector and national risk assessment, national cybersecurity capabilities, situational awareness and continuity of critical national services. Information sharing (chapter 5) links the three levels.

How do Always Applicable controls and the P1 to P4 priorities work?

Under the IA Regulation v1.1, section 3.3, an entity treats all controls as applicable until its risk assessment justifies excluding some, but the Always Applicable controls must be implemented regardless. Section 3.4 groups controls into four priority levels, P1 to P4, and critical entities begin with P1. P1 controls that apply may be augmented but never reduced.

How does NESA monitor compliance?

Section 7.2 describes four escalating levels: reporting, where NESA consolidates maturity-based self-assessments; auditing, where it may ask for evidence behind them; testing, where it can commission tests of security measures; and national security intervention in extreme cases. Each entity names a Liaison Officer for this contact under section 7.1.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

License included / downloadable: Yes The NIAF and the UAE Information Assurance Regulation v1.1 are published free by the UAE Government on u.ae and by TDRA. The platform links to the official pages and does not reproduce the text.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.