ManageEngine
EventLog Analyzer

UAE SIA (NESA)

compliance guide

www.eventloganalyzer.com

Index

What is UAE SIA (NESA)?

The UAE Signals Intelligence Agency (SIA)—formerly known as the National Electronic Security Authority (NESA)—is a federal authority that's responsible for enhancing cybersecurity policies and procedures in the United Arab Emirates (UAE). It was introduced in June 2014 to oversee the security and resilience of the UAE's critical information infrastructure and to ensure the implementation of effective cybersecurity measures.

The UAE Information Assurance (IA) Regulation (sometimes known as NESA regulatory compliance) is the set of management and technical controls to establish, implement, maintain, and enhance the nation's information security measures. The UAE IA Regulation is developed by the Telecommunications and Digital Government Regulatory Authority (often abbreviated to TRA) and it is a crucial component of the National Cyber Security Strategy (NCSS).

Complying with UAE IA Regulation is vital for maintaining national security, protecting critical infrastructure, securing sensitive information, mitigating legal and financial risks, and demonstrating a commitment to global information security standards. It contributes to a resilient and secure digital environment, benefiting both organizations within the UAE and the UAE as a whole.

Who must comply with UAE IA Regulation?

As per the UAE IA Regulation, all federal and local government entities, as well as critical infrastructure operators that provide essential services to the UAE—such as telecommunications, energy, transportation, and private sector companies that are designated as critical by the UAE government—are required to comply with UAE IA Regulation. However, the TRA highly recommends everyone adopt these regulations on a voluntary basis to achieve the goal of raising the nation's minimum security levels.

Consequences of UAE IA Regulation non-compliance

The IA Regulation sets out essential baseline requirements for protecting the critical information infrastructure of the United Arab Emirates. Although it has not specifically elaborated on penalties for non-compliance, not complying with the regulation can lead to increased scrutiny from regulators and the SIA/NESA. This may result in expensive audits, lawsuits, and the need for increased manpower.

In some cases, the UAE government can suspend the operations of an organization found to be in non-compliance with the IA Regulation. The government may also impose financial penalties on organizations that are found to be in non-compliance with the IA Regulation in accordance with the severity of the violation.

In addition to the legal consequences, non-compliance with the IA Regulation can also damage the organization's reputation and make it more vulnerable to cyberattacks.

UAE IA Regulation requirements for compliance

According to the official guideline of the UAE government, complying with UAE IA Regulation is based on four key elements: controls, sub-controls, performance indicators, and automation and implementation guidance for controls.

Controls:

All of the security controls specified in the UAE IA Regulation must be considered by each entity. Any entity that wants to claim compliance with the regulation must implement these controls based on the following requirements:

- **"Always Applicable" controls:** These controls are essential and must be implemented by any entity that wants to claim compliance with the UAE IA Regulation. Omitting any of these controls is not acceptable and will result in non-compliance.
- **Risk-based controls:** An entity must determine which of the security controls provided in the UAE IA Regulation are applicable to its particular situation based on the results of a risk assessment. Any controls that are excluded from the implementation plan must be justified and evidence must be provided, demonstrating that the associated risks have been accepted by accountable persons or authorizing entities.

The overall set of security controls that are "Always Applicable" and those security controls that have been determined as being applicable based on the risk assessment are "mandatory" for the entity to implement. These controls will be the basis of the compliance monitoring scheme.

Sub-controls:

While all the sub-controls of the "Always Applicable" security controls must be implemented, an entity may deviate from them if justified and appropriately supported. The acceptance of such deviations should be based on an informed decision-making process and risk assessment.

Performance indicators:

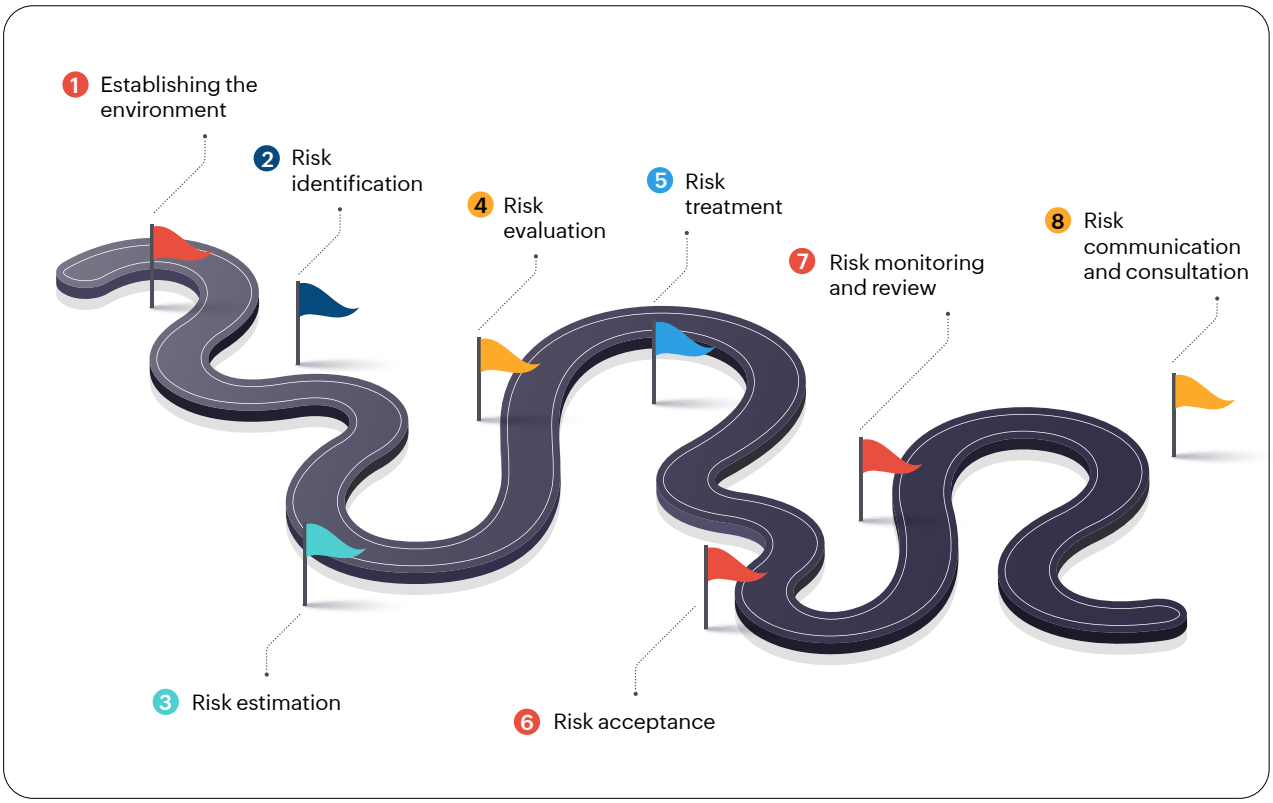
The UAE IA Regulation includes performance indicators that serve as basic guidelines for entities to assess the quality and effectiveness of their compliance with controls and control sub-families. While entities can deviate from these performance indicators, they are obligated to provide a justification for the deviation and specify new performance indicators if necessary.

Automation, Threat/Vulnerability Description for Sub-Families of Controls, and implementation guidance for controls:

The UAE IA Regulation includes performance indicators that serve as basic guidelines for entities to assess the quality and effectiveness of their compliance with controls and control sub-families. While entities can deviate from these performance indicators, they are obligated to provide a justification for the deviation and specify new performance indicators if necessary.

UAE IA Regulation roadmap

The UAE IA Regulation recommends adopting a risk-based approach while implementing the compliance. Following a risk-based approach ensures that the security controls are in accordance with the risk and magnitude in case of a potential breach. Performing risk management is the most crucial step toward implementing the regulation. Here are the 8 key activities mentioned in the UAE IA Regulation's risk-based approach.



Applicability of controls

Organizations have to identify the security controls that are mandatory to implement based on the list of applicable controls from the entity risk management process, apart from the "Always Applicable" controls. If there is no entity risk assessment then all the security controls are applicable and are mandatory for the implementation.

Prioritization of controls

The UAE IA Regulation framework organizes security controls in order of importance to ensure a minimum level of data protection. This prioritization is based on the impact that security controls have on safeguarding data. It helps organizations to:

- Mitigate common threats
- Build foundational IA capabilities

The security controls are categorized into four priority levels, namely P1, P2, P3, and P4. These priority levels are assigned in order of importance, with P1 being the highest priority and P4 being the lowest.

All critical entities implementing the UAE IA Regulation are required to implement all applicable security controls across the four priority levels. However, they should prioritize the implementation of P1 security controls, as these have the highest relative impact in protecting against critical threats and building foundational information assurance capabilities.

UAE IA Regulation best practices: A checklist

To achieve successful implementation of the UAE IA Regulation and related security controls, it is crucial to consider and adhere to the following essential factors mentioned in their guidelines:

1. Delivering awareness programs, training, and educational initiatives to ensure that all employees and stakeholders are well-informed about information assurance objectives
2. Developing a thorough understanding of information assurance requirements, which includes adopting a risk-based approach to identify relevant security controls and establish priorities for their implementation.
3. Adopting a tailored approach and framework to establish, implement, and improve information security that is consistent with the culture of the entity.
4. Gaining clarity on the methods used to assess and enforce compliance with the UAE IA Regulation.
5. Establishing a measurement system to monitor compliance, assess performance in information assurance management, and offer feedback and recommendations for enhancing and refining the UAE IA Regulation.
6. Escalating critical cybersecurity information to sector regulators (or equivalents) to enable the development of sector and national level views of risks.

7. Reporting critical cybersecurity information to sector regulators or equivalent entities to facilitate the creation of sector-specific and national-level risk perspectives.
8. Ensuring support and commitment from all levels of management.
9. Providing adequate funding for all information assurance activities.

UAE IA Regulation: Key controls to consider

For effective adoption and progression of the UAE IA Regulation, you should adhere to the security controls that are mandatory for implementation based on the list of applicable controls resulting from the entity risk assessment process.

The UAE IA Regulation's guidelines specifies security controls are organized into two categories: management controls and technical controls. The management controls are further divided into six families, while the technical controls are divided into nine families. Some of the key controls are in the table below.

Control families	Description
M1. Strategy and Planning	An information security strategy should be defined and an operating model is to be developed to adhere to the strategy. Information security plans should be developed for every major service to identify and mitigate risks.
M2. Information Securit Risk Management	An information security risk management process should be implemented. An awareness and training program should also be established.
M4. Compliance	Organizations should comply with legal requirements, security policies, and technical standards.
T1. Asset Management	Assets should be managed and information should be classified and labeled.
T.3 Operations Management	To ensure an appropriate level of information security, it is crucial to establish operational procedures and clearly define responsibilities.
T3.2.1	The entity shall develop recommended configuration settings for common information technology products.
T3.2.3	The entity shall control the changes to information systems.
T3.4.1	The entity shall protect its information assets from malware.
T3.6.3	The entity shall monitor the use of information systems.
T5.2.2	The entity shall restrict and control the allocation and use of privileges.

T5.4	To prevent unauthorized access to networked services
T.6 Third Party Security	Third-party security management should be done to ensure that third parties implement and uphold the necessary level of information security and service delivery.
T7.5.1	The entity shall control the installation of software on operational systems.
T7.5.2	The entity shall ensure the protection of system test data.
T7.5.3	The entity shall restrict the access to program source code.
T7.6.1	The entity shall control the implementation of changes by the use offormal change control procedures.
T7.7	To reduce risks resulting from exploitation of published or identified technical vulnerabilities
T8.3.2	The entity shall report information security events through appropriate management channels.

Compliance with UAE IA Regulations is imperative for organizations operating in the United Arab Emirates. It serves to enhance national security, protect critical infrastructure, safeguard sensitive information, foster trust, mitigate financial losses, and adapt organizations to the evolving threat landscape. By complying with Information Assurance Regulation guidelines, organizations play a vital role in strengthening the overall cybersecurity posture of the nation and ensuring a secure and resilient digital environment for all stakeholders.

Comply with UAE IA Regulation using EventLog Analyzer

EventLog Analyzer is a web-based IT compliance solution with real-time log management and network defense capabilities. The solution can provide your organization with the ability to dive deep into your machine logs and gain actionable insights. With EventLog Analyzer, your organization will be equipped to face diverse threats and protect critical client PHI while saving valuable time by generating predefined compliance reports. You can schedule a demo today and see for yourself how EventLog Analyzer makes it easy to comply with some of the most important mandates of UAE IA Regulation.

Our Products

AD360 | Log360 | ADAudit Plus | Exchange Reporter Plus | DataSecurity Plus | SharePoint Manager Plus

ManageEngine
EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

Download Demo