semperis

WHITE PAPER

Information Assurance Regulation

The IA Regulation and Your Identity Infrastructure

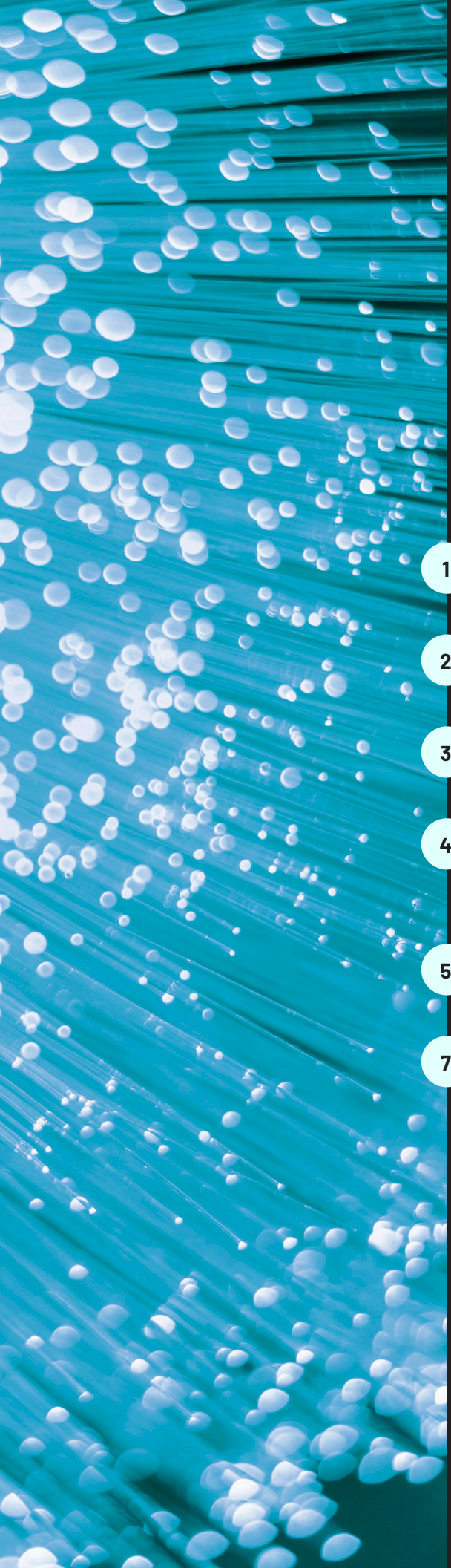


TABLE OF Contents

semperis

Introduction

The United Arab Emirates (UAE) Information Assurance (IA) Regulation is a set of controls developed to establish a minimum level of cybersecurity across information assets, practices, and standards for organisations operating in the UAE's digital space. Compliance is specifically required for *critical entities*—that is, organisations that operate critical infrastructure—but the regulation was developed to be universally applicable and is recommended for use by any entity to protect sensitive information, enhance security posture, and manage risks in a coordinated, systematic manner.

The IA Regulation emphasises key areas such as access control, incident response (IR), and data protection. Compliance with the required controls not only mitigates cybersecurity risks but also plays a crucial role in fostering national security, economic diversification, and trust in the nation's growing digital business and operational environment.

Prioritization of identity system security, recovery, and resilience is critical in meeting IA Regulation requirements. For 90% of organisations worldwide,[1] **Active Directory (AD)** is the identity system that provides centralized access control and identity management, making it a primary target for cyber attackers. Thus, the ability to respond quickly to AD threats and recover AD effectively after cyber incidents is crucial for maintaining the security and integrity of the UAE's critical entities.

By implementing strong AD security practices such as user account management, IR planning, system patching, encryption, and robust auditing, security teams fulfil the IA Regulation's cybersecurity objectives to "establish, implement, maintain, and continuously improve information assurance."[2]

1 A quarter century of control: The enduring power of Active Directory | Security Info Watch

2 UAE Information Assurance (IA) Regulation | The Official Portal of the UAE Government

The emerging threat landscape

The UAE government recognises a key challenge: While growth in the information technology (IT) space brings opportunities for innovation and global economic leadership, the cyber threat landscape is also evolving. As UAE entities thrive with greater digital transformation and rapid technology improvements, their increasing reliance on digital infrastructure unfortunately makes them a target.

Identity remains one of the main threat vectors for organised crime.[3] Password spraying attacks, weak passwords, unhardened access environments, and vulnerabilities in multifactor authentication configuration routinely give attackers an easy way in. In fact, Microsoft reported 7,000 identity-based attacks per second in 2024. Ninety-nine percent of them were password attacks.[4]

With even the smallest piece of information, most attackers target identity systems such as **AD and Entra ID** first. AD presents a large attack surface, and the complexity of its internal relationships makes misconfigurations and vulnerabilities hard to secure. Once AD is compromised, attackers can perform reconnaissance, seize control of data and assets, or launch attacks.

One of the highest profile attack types, **ransomware**, causes significant destruction while exposing sensitive personal and business data, enabling the extortion of millions of dollars—often multiple times.[5] Attackers gain access through social engineering or stolen credentials, then quickly pivot to the identity infrastructure, which provides controls for authentication and authorisation across most critical business systems.

Even a prolific ransomware actor like Akira,[6] which is otherwise known for leveraging perimeter device vulnerabilities, makes good use of the AD infrastructure, using tools such as Mimikatz and LaZagne to steal credentials, then creating new administrative accounts on domain controllers for persistence and lateral movement.

3 Ransomware Risk Report - Semperis

4 Microsoft Digital Defence Report 2024

5 Ransomware Risk Report - Semperis

6 Akira, GOLD SAHARA, PUNK SPIDER, Howling Scorpius, Group G1024 | MITRE ATT&CK®

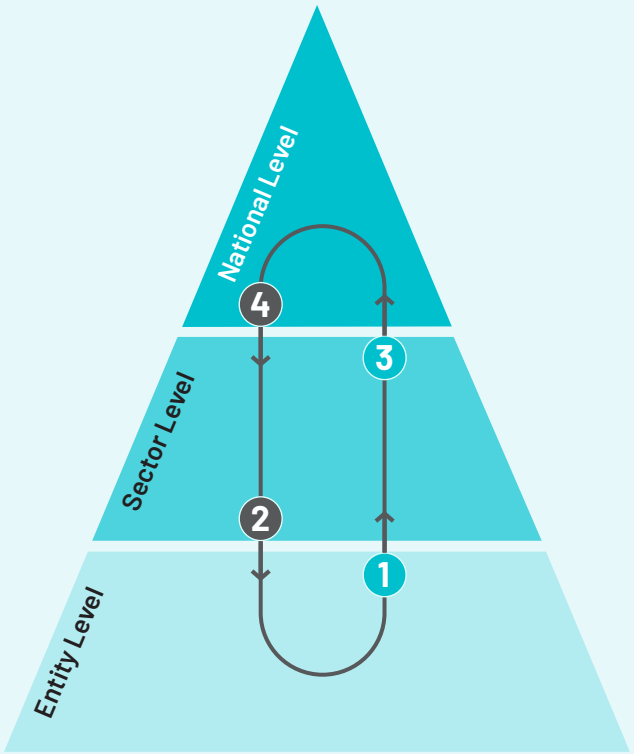
Scope of the UAE IA Regulation

Developed by the Telecommunications and Digital Government Regulatory Authority (TRA), the IA Regulation establishes a minimum security baseline for all implementing entities in the UAE.

TRA mandates compliance for all UAE government entities and other entities identified as critical. However, TRA highly recommends that all entities in the UAE adopt the controls on a voluntary basis, as applicable, to participate in raising the nation's overall security posture.

The IA Regulation is structured to enable information sharing and reporting across entities, industry sectors, and national organisations (**Figure 1**).

Figure 1. Information sharing and reporting on cybersecurity threats and mitigation strategies is integrated across UAE entities, industry sectors, and national organisations.



4 TRA consolidates and analyses the information reported by sector regulators to form a national and sector view on the state of the regulation implementation, as well as the risks, and shares relevant threat and risk information with sector regulators to increase effectiveness of the incident management and risk assessment programmes.

3 Sector regulators consolidate and analyse information reported by entities to form a sector view of risks and the state of the UAE IA Regulation implementation, and escalate key findings to TRA and other cybersecurity parties.

2 Sector regulators share relevant security threat, risk, and incident information with entities to increase effectiveness of the incident managment and risk assessment programmes.

1 Entities report key information to sector regulators, in particular relating to:

- State of the UAE IA Regulation implementation
- Risk assessment outcomes
- Cybersecurity threats, risks, and incidents

IA Regulation controls: Where to focus on identity

The UAE's regulation[7] draws on internationally recognised standards and incorporates best practices from the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), National Institute of Standards and Technology (NIST), the Abu Dhabi Information Security Standards, and SANS Institute.

The resulting comprehensive requirements promote a risk-based lifecycle approach that aims to enable entities to maintain current risk assessments; deal with their highest-priority risks in a timely way; and systematically identify, estimate, evaluate, and treat risks as they emerge.

In this paper, we won't review the entire regulation but highlight the **Management Controls (M)** and **Technical Controls (T)** that relate specifically to identity security. **These fall into the key control category areas shown in the following table.**

7 UAE Information Assurance (IA) Regulation | The Official Portal of the UAE Government

How can Semperis help?

Semperis leads the industry with Microsoft MVPs in AD and Entra ID recovery and resilience to ensure organisations have AD resilience built into their AD backup, recovery, and security plan. Semperis products, platforms, and services are enhanced by deep research from the AD-focused threat team.

Area	IA Regulation controls	How Semperis can help
Risk management and compliance	• M2.2.2 • M2.4.1 • M5.3.1	• Evaluate and communicate overall security posture with risk scoring, enabling drill-down into individual security categories for deeper analysis • Provide guidance for addressing security exposures at the strategic, operational, and tactical levels • Establish incident response and recovery planning and testing • Provide continuous threat and vulnerability detection
Indicators of exposure	• T3.2.1 • T3.2.5 • T7.7 • T8.3	• Monitor AD and Entra ID as a core dependency to all IT systems • Continuously monitor for indicators of exposure and compromise in AD and Entra ID using multiple data sources, including the AD replication stream • Discover attack paths to Tier 0 assets and help identify excessive privileges that attackers can exploit
Change control	• T3.2.3 • T7.6.1	• Provide comprehensive change tracking to identify identity system changes even with security logging turned off, if logs are deleted, agents are disabled or not working, or if changes are injected directly • Identify and automatically roll back suspicious, malicious, or unintended changes

Area	IA Regulation controls	How Semperis can help
Business continuity management **Environments management** **Backup** **Tested recovery**	• T3.3.2 – guidance f • T9.2.2 • T3.2.5 – guidance d • T3.5.1 • T3.4 – guidance f	• Automate identity system backups • Provide a full replica of identity systems in a development, test, or separate environment • Automate the complicated backup and recovery process for AD, including relevant dependencies, achieving up to 90% faster recovery • Provide proven, clean-state restore with validated recovery point objectives and recovery time objectives • Conduct bi-annual recovery drills
Logging and trustworthy monitoring	• T3.6.1 • T3.6.2 • T3.6.4	• Provide comprehensive logs and highly specialised AD and Entra ID threat analysis, enabling up-to-date, industry-leading insights, automation of identity security monitoring, and enrichment of SOC visibility through SIEM integration
Incident response and readiness	• T8.1.1 • T8.2.5 • T8.3	• Provide expert review of existing AD disaster recovery plan and expert guidance to protect identity systems before, during, and after an attack through Identity Forensics & Incident Response (IFIR) services • Centralize and unify all aspects of cyber crisis planning and incident response in the Ready1 platform, including process and procedure documentation, clarification of roles and responsibilities, secure communication across internal teams and external vendors, real-time status updates, plan testing and tabletop exercises, and incident forensics and reporting

Conclusion

The UAE IA Regulation requires significant measures to achieve compliance. To comply with the regulation, we recommend that you establish eight major capabilities for the resilience of your AD and Entra ID services:

1. Establish governance and ownership for your identity system.
2. Build visibility into risks and dependencies.
3. Establish comprehensive and automated exposure, threat, and vulnerability monitoring and integrate this capability into your SOC.
4. Remediate your identity vulnerabilities to reduce the attack surface for penetration testers and attackers alike.
5. Ensure you have the appropriate requirements and means of managing identity system risk in your supply chain.
6. Build robust response capabilities for your identity system to enable rapid IR, reporting, and forensic capabilities.
7. Have an automated and tested recovery process to enable rapid restoration in case of a destructive incident.
8. Establish a project of continuous improvement, including adopting best practices from the cybersecurity industry.

In our experience, achieving these capabilities is challenging. Sustaining them over time is not possible without significant automation. Semperis' market-leading products can provide you with this threat-led, automated capability.