FORTRA

DATASHEET (FORTRA)

Achieving UAE IA Compliance With Fortra

The UAE Information Assurance (IA) Standard provides requirements to raise the minimum level of protection of information assets and supporting systems across all implementing entities in the United Arab Emirates. It mandates a set of controls to protect UAE organizations' sensitive data through a framework that encompasses governance, classification, technical controls, continuous monitoring, and risk management.

Organizations need to comply with UAE IA policies, but they also need to take compliance a step further — they must have documented proof of continuous visibility, automated enforcement, auditability, and integrated security controls as part of their everyday business operations. The UAE IA contains six management control families and nine technical control families.

Fortra helps organizations operationalize UAE IA requirements through the integrated Fortra Data Security Platform. Fortra's data security solutions maximize visibility, data protection, and audit readiness while reducing risk across email, cloud, endpoints, collaboration platforms, and AI applications. Together, these solutions enable:

- Sensitive data discovery and inventory
- Information classification and labeling
- Data loss prevention and secure information transfer
- Encryption and persistent data protection
- Audit logging and incident investigation
- Data governance and compliance reporting
- Continuous monitoring and risk reduction

KEY BUSINESS BENEFITS

- Audit-readiness and regulatory reporting
- Data identification and classification
- Secure data processing, storage, and transfer
- Persistent automated encryption enforcement
- Insider threat and policy violation detection
- Reduced risk of unauthorized data transfers
- Cross-border data transfer restrictions

Requirements-to-Solution Mapping

REQUIREMENT	DETAIL	FORTRA CAPABILITY	BUSINESS OUTCOME
Information Classification (IA T1)	Control T1.3.1 requires organizations to develop an information classification scheme based on information value, legal and regulatory requirements, and sensitivity. It mandates that automated systems can access this classification to enforce specific protections.	Fortra Data Security Suite (DCS), Fortra Data Security Posture Management (DSPM)	User-driven classification, automated classification, visual markings, metadata tagging, headers, footers, watermarks and classification policies. Establishes consistent information handling practices and provides metadata that drives downstream security controls.
Information Transfer Security (IA T4)	Control T4.2.1 mandates formal transfer procedures and controls to protect the exchange of information from interception, mis-routing, or unauthorized disclosure.	Fortra Data Loss Prevention (DLP), Fortra Secure Email Gateway (SEG), Fortra Managed File Transfer (MFT)	Safe recipient checks, secure file transfer, email controls, transfer monitoring, encryption and authentication controls. Protects sensitive information during exchange and reduces risk of accidental disclosure.
Monitoring & Audit Logging (IA T3)	Control T3.6.2 requires comprehensive audit logging and maintaining evidence that supports security investigations and compliance reviews. The T8 family requires incident management documentation, situational awareness, and reporting of security weaknesses.	Fortra DCS, Fortra DLP, Fortra's Tripwire, Fortra DSPM	Detailed audit logs, classification events, file activity monitoring, SIEM integration, forensic evidence collection. Supports audit readiness, investigations, and continuous compliance monitoring.
Security Awareness and Training (M3.3 & M3.4)	Control M3.3 requires organizations to implement and track security training. M3.4 requires ongoing security awareness to reinforce cyber risk awareness and secure behaviors.	Fortra Security Awareness Training	Provides role-based security training and maintains an ongoing security awareness program with measurable effectiveness, including phishing simulations, assessments, and audit-ready reporting to improve user awareness and demonstrate compliance.
Compliance with Technical Requirements (M5.4)	Control M5.4 requires organizations to implement and continuously monitor technical security controls to ensure compliance with information security requirements.	Fortra's Tripwire, Fortra VM	Continuously monitors technical security controls and system configurations, detects unauthorized changes, identifies vulnerabilities, and provides audit-ready reporting to maintain compliance with information security requirements.