ITSEC

VARA Compliance Map

Complete Guide to Technology & Information Rulebook Requirements for Virtual Asset Service Providers

Effective: 19 May 2026

Executive Summary

Understanding VARA compliance requirements for virtual asset operations in Dubai

What is VARA Compliance?

The Virtual Assets Regulatory Authority (VARA) is Dubai's dedicated regulator for virtual assets and related activities. VARA's Technology & Information Rulebook establishes comprehensive cybersecurity and technology governance requirements that all licensed Virtual Asset Service Providers (VASPs) must implement and maintain.

Key Insight: VARA compliance is not optional. Non-compliant entities face license suspension, revocation, and significant financial penalties. The rulebook mandates annual independent security assessments and continuous monitoring.

Who Needs VARA Compliance?

The following entities operating in Dubai must obtain VARA authorization and comply with the Technology & Information Rulebook:

🏛 Crypto Exchanges	🔐 Custody Providers
🔄 Broker-Dealers	💳 Payment Services
📊 Advisory Services	💰 Lending Platforms
🪙 Token Issuers	📱 Wallet Providers

⚠️ **Non-Compliance Consequences:** Failure to meet VARA requirements can result in license suspension or revocation, substantial financial penalties, reputational damage, and prohibition from operating in Dubai's virtual asset market.

Core Requirements Matrix

VARA Technology & Information Rulebook requirements mapped to ITSEC solutions

#	Rulebook	Requirement	Description	ITSEC Solution
1	Rule E	Red Team Simulation (TLPT)	Annual independent threat-led penetration testing by qualified third-party assessors	Threat-Led Penetration Testing
2	Rule F	Continuous Monitoring	Quarterly security audits, vulnerability scanning, and real-time threat detection	Automated Threat Detection
3	Rule D	Key Lifecycle Governance	Cryptographic key management, HSM integration, and secure key storage protocols	HSM Integration & Secure Storage
4	Rule I	CISO Appointment	Designated Chief Information Security Officer with documented responsibilities	Virtual CISO Services
5	Rule H	Incident Response	72-hour notification to VARA, incident management, and business continuity	BCDR & Response Planning
6	Rule G	Access Controls	Multi-factor authentication, role-based access, and privileged access management	IAM Policies & Audit Trails

ITSEC Advantage: Our comprehensive compliance packages address all six core requirements with proven methodologies, ensuring first-attempt audit success and ongoing regulatory alignment.

Extended Requirements Matrix

Additional technology and information security controls required by VARA

#	Rulebook	Requirement	Description	ITSEC Solution
7	Rule B	IT Governance	Documented IT policies, procedures, and governance frameworks	Policy Development
8	Rule C	Risk Management	Technology risk assessment and management frameworks	Risk Assessment Services
9	Rule J	Third-Party Risk	Vendor due diligence and third-party security assessments	Vendor Security Audit
10	Rule K	Data Protection	Data classification, encryption, and protection controls	Data Security Framework
11	Rule L	Change Management	Controlled change management for systems and infrastructure	Change Control Advisory
12	Rule M	Asset Management	IT asset inventory and lifecycle management	Asset Discovery & CMDB

Documentation Requirements

VARA requires comprehensive documentation including information security policies, access control procedures, incident response plans, business continuity plans, and annual audit reports.

Reporting Obligations

Licensed VASPs must submit annual compliance reports, notify VARA of security incidents within 72 hours, and maintain audit trails for a minimum of 5 years.

Your Path to VARA Compliance

ITSEC's proven 5-step methodology gets you audit-ready in 4-6 weeks

Day 1

Initial Consultation

Comprehensive discovery session to understand your operations, current security posture, and VARA license category requirements.

Days 2-5

Gap Assessment

Detailed analysis of your current state against all VARA Technology & Information Rulebook requirements. Deliverable: Gap Assessment Report with prioritized findings.

Weeks 1-2

Red Team Simulation (TLPT)

Independent threat-led penetration testing covering web applications, APIs, mobile apps, and infrastructure. Identifies vulnerabilities before VARA audit.

Weeks 2-4

Remediation & Documentation

Fix identified vulnerabilities, develop required policies and procedures, implement technical controls, and prepare evidence packages.

Weeks 4-6

Audit Preparation & Support

Mock audits, evidence collection, auditor coordination, and on-site support during the official VARA security assessment.

> ✓ **Final Outcome:** VARA License Approved — Start operating in Dubai's regulated virtual asset market with full compliance.

Entity-Specific Requirements

Tailored security solutions for each VARA license category

Exchange Services

✓ Red Team / TLPT Assessment
✓ Hot & Cold Wallet Security
✓ SOC Integration & Monitoring
✓ Trading Engine Security

Broker-Dealer

✓ Trading Platform Security
✓ API Security Testing
✓ Order Management Controls
✓ Client Data Protection

Custody Services

✓ Vault Security Architecture
✓ Key Management & HSM
✓ Asset Transfer Controls
✓ Multi-Signature Protocols

Lending/Borrowing

✓ Smart Contract Security
✓ Oracle Security Review
✓ Collateral Management
✓ Liquidation Mechanism Audit

Management/Investment

✓ Portfolio Platform Security
✓ Fund Administration Controls
✓ Reporting System Integrity
✓ Investor Data Protection

VA Issuance

✓ Smart Contract Audit
✓ Key Custody Solutions
✓ Issuance Platform Security
✓ Token Economics Review

Customized Approach: Each VARA license category has specific requirements. ITSEC tailors our assessment methodology to address the unique security challenges of your business model.

VARA Compliance Checklist

Self-assessment checklist for VARA Technology & Information Rulebook requirements

☐ Information Security Policy documented and approved

☐ Chief Information Security Officer (CISO) appointed

☐ Annual TLPT/Red Team assessment completed

☐ Quarterly vulnerability scanning implemented

☐ Multi-factor authentication (MFA) enabled

☐ Role-based access controls implemented

☐ Cryptographic key management procedures

☐ HSM integration for key storage

☐ Incident response plan documented

☐ 72-hour VARA notification process established

☐ Business continuity plan in place

☐ Disaster recovery procedures tested

☐ Data classification framework implemented

☐ Encryption at rest and in transit

☐ Third-party vendor security assessments

☐ Change management procedures documented

☐ IT asset inventory maintained

☐ Security awareness training completed

☐ Audit trail retention (5+ years)

☐ Annual compliance report prepared

⚠ **Important:** This checklist is for self-assessment purposes. A qualified independent assessor must verify compliance for VARA licensing. Contact ITSEC for a comprehensive gap assessment.

ITSEC

Why Choose ITSEC

UAE's most trusted VARA compliance partner with 100% audit success rate

🏆	📜	🔒	🇦🇪
100% Audit Success Rate	**ISO 27001 Certified**	**CREST Accredited**	**UAE Licensed Since 2011**

📞	🔢	✉️
Phone	Mobile	Email
+971.4.257.2406	**+971.52.509.7278**	**hello@itsecnow.com**

Ready to Get VARA Compliant?

Schedule your free VARA Readiness Assessment with our crypto security experts today.

Request Assessment →

▍Our Expertise

25+ VARA clients served with zero failed audits. Our team includes 50+ crypto security specialists with deep expertise in exchange security, smart contracts, and regulatory compliance.

▍Fast-Track Process

Our optimized methodology gets you VARA-ready in 4-6 weeks. Parallel workstreams, dedicated project managers, and proven templates accelerate your compliance journey.