Gulf Cybersecurity Regulations at a Glance

Five Regulatory Frameworks | Five Jurisdictions



Saudi Arabia

SAMA
Cyber Security Framework

Regulator:
Saudi Central Bank (SAMA)

Applies to:
SAMA-regulated financial institutions.

Core Requirements:
- Cybersecurity governance
- Cyber risk management
- Identity and access control
- Security monitoring and incident response
- Third-party risk management

Saudi Arabia

NCA
Essential Cybersecurity Controls (ECC 2-2024)

Regulator:
National Cybersecurity Authority (NCA)

Applies to:
Government entities and organisations within scope, including critical infrastructure.

Core Requirements:
- Cybersecurity governance
- Risk and asset management
- Vulnerability management
- Cloud and infrastructure security
- Incident response and business continuity

UAE

IA
Information Assurance Regulation

Authority:
Telecommunications and Digital Government Regulatory Authority (TDRA)

Applies to:
Designated government and critical information infrastructure entities.

Core Requirements:
- Information security governance
- Risk assessment
- Data and asset protection
- Access control
- Security monitoring and compliance

Qatar

NIA
National Information Assurance Standard

Authority:
National Cyber Security Agency (NCSA)

Applies to:
Organisations within the standard's defined scope.

Core Requirements:
- Information security governance
- Risk management
- Data classification and protection
- Access and cryptographic controls
- Incident management
- Business continuity

Bahrain

CBB
Cybersecurity Requirements

Regulator:
Central Bank of Bahrain (CBB)

Applies to:
CBB-licensed financial institutions.

Core Requirements:
- Cybersecurity risk management
- Vulnerability assessments and penetration testing
- Security monitoring
- Incident reporting
- Business continuity
- Third-party security

www.ampcuscyber.com | letsconnect@ampcuscyber.com