SECUREYES
Infusing Security

CYBERSECURITY GUIDELINES FOR BANKS

ACROSS WEST ASIA

SAUDI ARABIA

BAHRAIN

EGYPT

IRAQ

UNITED ARAB EMIRATES

KUWAIT

QATAR

A concise cybersecurity guide **for banks across West Asia.**

This guide is designed for Chief Information Security Officers (**CISO**s), Chief Risk Officers (**CRO**s), Chief Compliance Officers (**CCO**s), **GRC Heads**, and **IT Heads** of banking institutions across West Asia.

As custodians of financial security and regulatory compliance, these professionals face an ever-evolving landscape of cyber threats, regulatory mandates, and operational challenges.

This guide helps safeguard sensitive data, strengthen risk management strategies, and build a robust cybersecurity posture to mitigate emerging threats effectively.

What this guide covers:

- **Saudi Arabia:** SAMA Cybersecurity Guidelines
- **Bahrain:** Central Bank of Bahrain (CBB) Cybersecurity Framework
- **Iraq:** Central Bank of Iraq (CBI) Cybersecurity Regulations
- **Egypt:** Central Bank of Egypt (CBE) Cybersecurity Standards
- **Kuwait:** Central Bank of Kuwait (CBK) Cybersecurity Framework
- **Qatar:** Qatar Central Bank (QCB) Cybersecurity Mandates
- **United Arab Emirates:** Central Bank of UAE (CBUAE) Cybersecurity Guidelines
- Implementation **Best Practices** for Banking Institutions
- **Strategic Recommendations**

Saudi Arabia

The Saudi Central Bank (SAMA) Guidelines

Key Policy Document:

- SAMA Cybersecurity Framework
- IT Governance Framework
- Counter-Fraud Framework

Key Requirements:

- Establishment of a Saudi-national Chief Information Security Officer (CISO)
- Cybersecurity maturity model (minimum level 3 compliance)
- Mandatory third-party cybersecurity controls
- Red teaming exercises every three years
- Real-time security monitoring and incident response

Additional Considerations:

- Banks must seek approval from SAMA for cloud computing solutions.
- Periodic audits are required to evaluate the effectiveness of cybersecurity measures.
- Compliance with international standards such as ISO 27001 and NIST.

Action Plan for Cybersecurity Compliance

Step 1: Governance and Leadership

- Define a cybersecurity strategy aligned with SAMA's objectives.
- Develop and endorse a cybersecurity governance structure.

Step 2: Risk Management

- Conduct periodic risk assessments of information assets.
- Define the organization's risk appetite and mitigation strategies.

Step 3: Operations and Technology

- Implement robust identity and access management protocols.
- Establish monitoring systems for threat detection and vulnerability management.

Step 4: Third-Party Security

- Mandate cybersecurity controls for all third-party vendors.
- Obtain SAMA approval for cloud service usage.

Step 5: Awareness and Training

- Conduct regular cybersecurity training for employees, vendors, and customers.
- Promote a security-aware culture through awareness programs.

Bahrain

Central Bank of Bahrain (CBB) Cybersecurity Framework

Key Policy Document:

- CBB Cybersecurity Risk Management Framework

Governance and Oversight:

- Board Responsibilities: The Board of Directors is accountable for cybersecurity strategy, ensuring adequate budget allocation, and approving risk management frameworks. Cybersecurity must be a regular topic at board meetings.
- Senior Management: Responsible for implementing the cybersecurity risk management framework and monitoring its effectiveness. This includes classifying information assets, ensuring adequate staffing, and providing periodic reports to the board.
- Cybersecurity Committee: Chaired by a senior independent manager, this committee oversees cybersecurity policies and frameworks.

Incident Response, Business Continuity, Third-Party and Trainings:

- Incident Response Framework: Develop and maintain an incident response plan that includes detection, containment, recovery, and reporting. Test response readiness through regular drills and tabletop exercises. Establish a dedicated incident handling team with clear roles and responsibilities.

- Incident Classification and Reporting: Categorize incidents based on severity (low, medium, high) using a pre-defined taxonomy. Report medium and high-severity incidents to the CBB immediately. Maintain detailed records of all incidents in a centralized repository.

- Business Continuity and Disaster Recovery (BC/DR): Develop a comprehensive BC/DR plan to ensure mission-critical operations continue during disruptions. Conduct business impact analyses to prioritize recovery objectives. Test disaster recovery plans regularly, including restoring from offline backups.

- Third-Party Cybersecurity: Conduct detailed feasibility studies to identify cybersecurity risks in outsourcing agreements. Ensure contracts include confidentiality, integrity, and availability clauses. Regularly audit third-party compliance with cybersecurity requirements.

- Cybersecurity Awareness and Training program for employees, third parties, and customers. Provide role-specific training, update training programs annually to address emerging threats and compliance requirements.

Iraq

Central Bank of Iraq (CBI) Cybersecurity Regulations

Key Policy Document:

- CBI Cybersecurity Regulatory Framework

Risk Management Practices

- Maintain a dedicated risk management department. Identify, assess, and document risks in a centralized risk register. Regularly review risk tolerance levels and mitigation strategies.

Business Continuity Planning

- Develop business continuity plans aligned with international standards. Conduct regular impact assessments to establish recovery objectives. Test recovery procedures to ensure resilience during disruptions.

Operational Controls and Cyber Defence:

- Asset Inventory: Maintain an up-to-date inventory of all information assets.
- Data Classification: Categorize data based on sensitivity and establish clear ownership.
- Access Controls: Implement multi-factor authentication and role-based access permissions.

Cyber Defence Mechanisms

- Vulnerability Management: Perform regular assessments and apply security patches promptly.
- Penetration Testing: Conduct tests to identify weaknesses in systems and applications.
- Threat Intelligence: Utilize cyber threat intelligence services to stay ahead of emerging risks.

Cybersecurity Awareness and Training

- Conduct regular cybersecurity training for employees, third parties, and stakeholders. Develop role-specific programs for executives, IT staff, and compliance officers.

Third-Party Security

- Conduct thorough due diligence before engaging third-party vendors. Include cybersecurity clauses in all contracts, emphasizing confidentiality and data protection. Monitor vendor compliance with CBI's cybersecurity standards.

Egypt

Central Bank of Egypt (CBE) Cybersecurity Standards

Key Policy Documents:

- Egypt Financial Cybersecurity Framework (EGY-FIN CSF)
- Personal Data Protection Law (Law No. 151 of 2020)

Cybersecurity Framework (EGY-FIN CSF)

- Flexibility in Implementation: Licensed entities can customize controls aligned with industry best practices.
- Structured Assessment: Use CBE's maturity models for consistent evaluation and improvement.
- Risk Appetite and Strategy: Define organizational risk tolerance and align cybersecurity goals with strategic priorities.

Data Protection and Compliance Laws

- Personal Data Protection Law (Law No. 151 of 2020): Safeguards individual privacy and mandates robust data management.
- Anti-Cyber and IT Crimes Law (Law No. 175 of 2018): Imposes penalties for unauthorized access and data breaches.

Actionable Steps for Compliance:

- Appoint a dedicated Chief Information Security Officer (CISO) with clear reporting lines.
- Identify vulnerabilities and prioritize mitigation strategies.
- Asset management for physical, digital, and cybersecurity-centric resources.
- Develop a business resilience strategy based on Business Impact Analysis (BIA).
- Conduct annual simulation exercises to test response plans.
- Ensure vendors comply with cybersecurity controls and conduct periodic audits.
- Implement network security protocols for third-party connections.
- Security Awareness: Regular training for employees, contractors, and third parties.
- Endpoint Security: Protect against malware, ransomware, and unauthorized access.
- Application Security: Mitigate risks in software applications
- Network Security: Secure data in transit using encryption and access controls.
- Implement Identity and Access Management (IAM)
- Deploy a Security Operations Center (SOC) for real-time threat monitoring.
- Use Cyber Threat Intelligence (CTI) to identify and respond to emerging risks.
- Conduct patch and vulnerability management to address system weaknesses.
- Perform independent audits of IT governance and cybersecurity processes.
- Maintain documentation of incident reports, risk assessments, and compliance findings.
- Submit periodic compliance reports to the CBE.
- Red Team Exercises: Conduct ethical hacking exercises to evaluate security preparedness. Use findings to improve defense mechanisms and incident response protocols.

Kuwait

Central Bank of Kuwait (CBK) Cybersecurity Framework

Key Policy Documents:

- CBK Cybersecurity Framework (CSF)

Governance: Accountability lies with the Board of Directors and Senior Management. Boards must receive periodic updates on cybersecurity programs, incidents, and risks.

Risk Management: Conduct regular cyber risk assessments. Maintain a risk register prioritizing mitigation strategies.

Compliance Requirements

- Adhere to laws such as CBK Law 32 (1968) and Law 20 (2014).
- Align with international standards (ISO 22301, ISO 31000, and SWIFT CSCF).
- Conduct independent audits every two years to evaluate cybersecurity effectiveness.

Cybersecurity Strategy and Policy

- Develop a cybersecurity strategy tailored to the organization's objectives.
- Establish policies addressing principles outlined in CBK's cybersecurity baselines.
- Ensure policies are communicated to employees and third parties.

Technology and Infrastructure Security

- Implement measures to mitigate malware, ransomware, and denial-of-service attacks.
- Secure external network connections with encryption and authentication protocols.

Incident Response Framework

- Cover detection, containment, recovery, and reporting. Test response readiness through regular tabletop exercises.
- Categorize incidents as low, medium, or high severity based on impact. Notify CBK immediately of medium and high-severity incidents.

Third-Party and Cloud Security

- Include security requirements in all third-party contracts.
- Monitor third-party compliance with CBK's cybersecurity standards.
- Define policies for cloud service usage, ensuring encryption and data logging.

Qatar

Qatar Central Bank (QCB) Cybersecurity Mandates

Key Policy Documents:

- QCB Technology Risks Circular 2018
- Information and Cybersecurity Regulations for PSPs

Establish a Cybersecurity Function

- Create a dedicated cybersecurity team led by the CISO.
- Integrate cybersecurity into the bank's strategic and operational plans.

Develop Policies and Procedures

- Document security policies and incident response plans.
- Align with QCB regulations and global standards.

Conduct Regular Risk Assessments

- Perform semi-annual vulnerability assessments and penetration testing.
- Maintain a dynamic risk register.

Security Awareness Training

- Train employees and stakeholders on cybersecurity best practices.
- Conduct phishing simulation exercises and regular updates on emerging threats.

Establish a 24/7 Security Operations Center (SOC)

- Centralize monitoring of cybersecurity threats.
- Use automated tools for intrusion detection and anomaly monitoring.

Reporting and Monitoring

- Submit annual compliance reports to QCB.
- Maintain logs and audit trails for at least six months.

Vendor Management

- Assess and monitor third-party service providers' compliance with QCB standards. Conduct independent audits of vendors regularly.

Cloud Computing and Data Localization

- Seek QCB approval for cloud services.
- Ensure data is stored and secured within Qatar.

Continuous Monitoring

- Use real-time monitoring tools for critical networks and applications.
- Implement threat intelligence platforms to detect and mitigate zero-day vulnerabilities.

Policy Reviews and Updates

- Regularly review and update cybersecurity policies.
- Stay informed about regulatory changes and industry best practices.

Simulated Drills and Exercises

- Conduct annual drills to test business continuity and incident response effectiveness.
- Engage with third-party experts for unbiased assessments.

United Arab Emirates

Central Bank of UAE (CBUAE) Cybersecurity Guidelines

Key Policy Documents:

- CBUAE Information Security Regulations
- UAE Information Assurance Standards

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Cybersecurity Governance: Assign a dedicated cybersecurity lead to oversee strategy and operations. Establish security administration processes to control access rights and monitor compliance.

Incident Response and Reporting: Develop a comprehensive incident response plan to isolate and neutralize threats. Ensure timely reporting of security breaches, fraud, and service disruptions to CBUAE.

Third-Party Risk Management: Vet third-party vendors for compliance with cybersecurity standards. Monitor cloud service providers and obtain necessary approvals from CBUAE. Regularly audit vendors for adherence to contractual obligations.

Cybersecurity Awareness and Training: Launch awareness campaigns targeting employees, vendors, and customers. Conduct phishing simulations to educate staff about social engineering attacks.

Anti-Fraud Measures: Establish fraud detection systems with multi-factor authentication for high-risk transactions. Maintain a centralized register for fraud incidents and monitor suspicious activities. Report fraud cases involving losses above AED 100,000 to relevant authorities.

AML/CFT Program: Develop a robust AML/CFT framework with policies approved by senior management. Appoint a full-time Compliance Officer, with no objection from CBUAE. Conduct KYC processes to verify customer identities using Emirates ID validation.

Independent audits: Audit AML/CFT functions and submit findings to CBUAE. Deploy advanced network monitoring tools, such as SIEM platforms. Monitor compliance with UAEFTS for local transactions.

Auditing and Documentation: Conduct bi-annual compliance audits and submit reports to CBUAE. Maintain comprehensive documentation of security controls, risk assessments, and audit outcomes. Ensure IT disaster recovery and backup plans are well-documented and tested.

Red Team Exercises: Perform ethical hacking and red teaming exercises to test resilience. Use insights from these exercises to strengthen incident response.

Best practices for banks.

Governance and Leadership

- Establish a dedicated Cybersecurity Governance Committee.
- Ensure board-level oversight of cybersecurity initiatives.
- Assign a Chief Information Security Officer (CISO) with direct reporting lines to senior leadership.

Risk Management and Compliance

- Conduct periodic risk assessments and implement a continuous improvement approach.
- Align cybersecurity policies with international frameworks such as ISO 27001, NIST, and PCI DSS.
- Implement comprehensive third-party risk management protocols.

Technology and Security Controls

- Deploy Security Information and Event Management (SIEM) systems for real-time monitoring.
- Enforce zero-trust security models with strong identity & access management (IAM).
- Utilize AI-powered threat intelligence to proactively mitigate risks.
- Secure cloud computing environments with encryption and multi-factor authentication.

Awareness and Training

- Conduct regular cybersecurity awareness programs for employees, customers, and third parties.
- Simulate phishing attacks and social engineering exercises to evaluate preparedness.
- Foster a culture of cybersecurity awareness across all organizational levels.

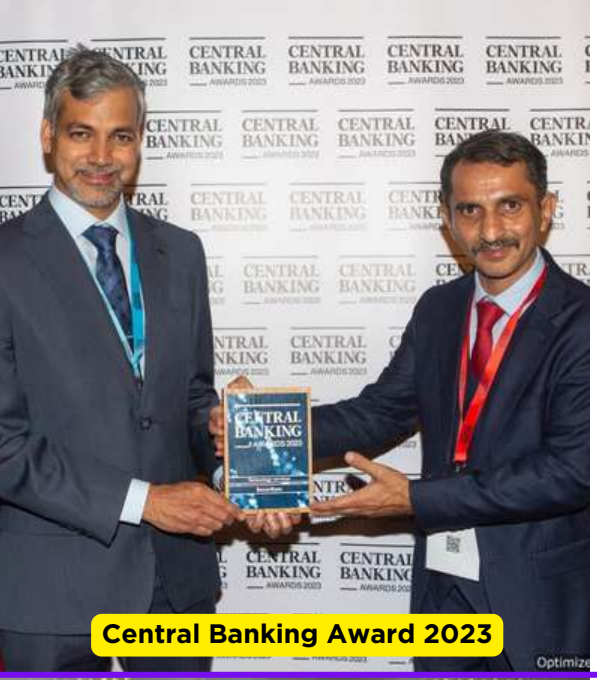
Incident Response and Business Continuity

- Develop and test a robust incident response plan.
- Conduct cyber resilience drills, including red teaming and breach simulation exercises.
- Establish an independent Security Operations Center (SOC) to detect and respond to threats in real-time.

SecurEyes

SecurEyes is a global leader in cybersecurity, empowering organizations to protect their digital assets, ensure compliance, and stay ahead of evolving threats.

With **18** years of expertise, cutting-edge tools, and tailored consulting services, we've earned the trust of governments, regulators, and Fortune 500 companies worldwide.



Central Banking Award 2023

ET Achievers Award 2022

Diverse Clientele

700+ happy clients across diverse industries. Here are a few of them.

WEST ASIA & NORTH AFRICA

Saudi Central Bank · Strategic Partnerships · GIB · Etihad Airways · The Saudi Investment Bank · RasGas · RAKBANK · SIMAH · Al Rajhi Bank · Emirates NBD · Ahlibank · tamam

ASIA PACIFIC

SBI · ICICI Bank · Canara Bank · India Post · HAL Hindustan Aeronautics Limited · Bharti AXA · NIC National Informatics Centre · Ministry of Home Affairs · Ministry of Finance · MyGov · Ministry of MSME, Govt. of India

NORTH AMERICA

Goldman Sachs · Brocade · EvalueServe · RSA Security · NTT Data · GNAX · Walmart · UNISYS · iQUANTI

Accreditations

CERT-In, NIC, ISO 9001:2015, and ISO 27001:2013 certified

250,000+

IPs covered under Penetration Testing.

10,000+

People covered under Social Engineering

30,000+

Servers reviewed

20,000+

Professionals trained

SECUREYES
Infusing Security

Let's Explore Synergies

Are you ready to transform your organization's cybersecurity posture?

Let's connect for a quick chat?

- Explore case studies
- Request policy/framework consultation
- Request product demo

https://calendly.com/hello-secureyes

www.secureyes.net

hello@secureyes.net

IND +91 9939217654
IND +91 8041264078
UAE +971 50 8950797
USA +1 361 423 1683