Kiteworks

GUIDE

Compliance Guide to Securing Sensitive Content in Qatar's Banking Sector

How the Kiteworks Private Content Network Helps Banks Meet Qatar Central Bank Technology Risks Requirements

Introduction

The Qatar Central Bank (QCB) Technology Risks circular of 2018 establishes comprehensive cybersecurity and technology risk management requirements for banks operating in Qatar. This regulatory framework aims to enhance the financial sector's cyber resilience and protect vital banking functions from emerging digital threats that could disrupt financial stability. The circular applies to all banks in Qatar and covers multiple aspects of technology risk management, including cybersecurity governance, IT operations, enterprise security, business continuity, and fraud prevention. Banks must implement robust cybersecurity frameworks with board-level oversight, maintain dedicated information security teams led by a Chief Information Security Officer (CISO), and conduct regular risk assessments and audits. The regulation mandates specific controls for network security, access management, data protection, and incident response.

Key provisions include the requirement for banks to establish 24/7 Security Operations Centers (SOCs), implement two-factor authentication for critical systems, and maintain data centers within Qatar. Banks must perform vulnerability assessments and penetration testing semiannually, encrypt sensitive data, and comply with international standards like PCI DSS for payment card security. The circular also requires banks to develop comprehensive incident response plans and report significant security incidents to QCB within one hour of detection. The regulation addresses emerging risks such as cloud computing, mobile banking, and third-party service providers. Banks must obtain QCB approval before engaging in cloud services or significant outsourcing arrangements. They must also implement strong controls for ATM security, payment card protection, and fraud prevention across all digital channels. Noncompliance with this regulation exposes banks to various risks, including regulatory penalties, reputational damage, and potential cyberattacks that could lead to financial losses and operational disruptions. The circular aligns with international standards such as ISO 27001:2013, NIST Cybersecurity Framework, and Qatar's National Information Assurance Partnership (NIAP) v2.0.

To comply, banks must maintain documented policies and procedures, conduct regular employee training, perform annual compliance assessments, and submit reports to QCB. They must also establish board-level oversight of technology risks, maintain adequate budgets for cybersecurity initiatives, and ensure proper segregation of duties between IT and security functions. This regulation reflects Qatar's commitment to maintaining a secure and resilient financial sector as part of its broader economic development goals. It recognizes the interconnected nature of the global financial system and implements controls to address both local and international cyber threats. The requirements complement other QCB regulations on banking supervision and align with Qatar's broader cybersecurity strategy.

This guide showcases how Kiteworks can support organizations looking to be compliant with the Qatar Central Bank (QCB) Technology Risks circular of 2018.

The Kiteworks Secure File Sharing and Governance Platform

The Kiteworks Private Content Network empowers organizations to share sensitive content with trusted parties by email, file sharing, file transfer, and other channels at the highest levels of security, governance, and compliance while maintaining full visibility and control over their file sharing activities. The Kiteworks platform provides:

ISO 27001 Certification

Kiteworks' ISO 27001 certification provides a validated framework for protecting sensitive financial data and managing IT risks in alignment with QCB's standards. The platform's established security governance, processes, and controls, including regular security audits, can help banks support compliance with QCB's cybersecurity requirements.

Protection of Unstructured Data

Kiteworks provides comprehensive protection for unstructured data through its advanced content firewall and zero-trust file sharing capabilities that ensures sensitive unstructured data remains secure throughout its life cycle, whether at rest or in transit across various communication channels.

Governance and Compliance

Kiteworks reduces compliance risk and cost by consolidating advanced content governance capabilities into a single platform. Whether employees send and receive content via email, file share, automated file transfer, APIs, or web forms, it's covered.

Simplicity and Ease of Use

Kiteworks offers a user-friendly interface that simplifies secure file sharing and collaboration, enabling users to easily send, receive, and manage sensitive content without compromising security. The platform's intuitive design and seamless integration with existing workflows ensures high user adoption rates and minimizes the learning curve for organizations implementing robust data protection measures.

The Kiteworks Platform and Qatar Central Bank Technology Risks

Chapter 1: Cyber Security Within the Organization

This chapter outlines the foundational requirements for cybersecurity governance in Qatar's banking sector. It mandates that banks establish a dedicated cybersecurity function with board oversight, appoint a CISO independent from IT operations, and maintain a comprehensive security program. The requirements emphasize regular risk assessments, policy reviews, and monitoring of key security indicators. Banks must create an Information Security Committee and ensure adequate resources for security operations.

Chapter Requirements	Kiteworks Solution
Qatar banks must implement comprehensive technical controls including robust identity and access management systems, security incident monitoring capabilities, and regular system security reviews. The requirements mandate implementation of audit trails and log monitoring systems to track system activities, along with regular integrity checks of system configurations. Banks must develop a security architecture aligned with their business strategy, which includes monitoring tools for security incidents and systematic assessment processes. These controls must be regularly reviewed and validated through the bank's information security program.	Kiteworks helps Qatar banks meet QCB's technical control requirements through its ISO 27001-certified platform's comprehensive security features. For identity and access management, Kiteworks offers multiple authentication methods including MFA, SAML 2.0 SSO, and Active Directory integration. Its security monitoring capabilities include intrusion and anomaly detection with pattern-based suspicious activity monitoring, while comprehensive SIEM-integrated audit logs enable thorough security incident review and system configuration monitoring. The platform's security architecture supports compliance through standardized, normalized log data aggregation for security and compliance activities, along with robust authentication controls including PIV/CAC cards and time-based OTP. These features help banks maintain the systematic security monitoring and access controls required by QCB regulations.

Chapters 2-5: Cyber Security in the Human Resources (HR), Legal and Compliance, Procurement, and Risk Departments

These chapters outline comprehensive cybersecurity requirements across HR, Legal/Compliance, Procurement, and Risk departments in Qatar's banking sector. The HR section focuses on personnel security and training programs, while Legal/Compliance emphasizes audit requirements and regulatory compliance. The Procurement chapter mandates vendor security assessment and management, and the Risk section establishes frameworks for identifying, assessing, and monitoring technology risks across the organization.

Chapter Requirements	Kiteworks Solution
Banks must implement comprehensive technical controls across multiple areas. For data protection, systems must enable encryption, access controls, and monitoring of all PII handling. Visitor management requires electronic tracking systems with automated logging and badge generation. Access management systems must support automated provisioning/de-provisioning and enforce least-privilege principles, while monitoring systems must detect unauthorized access and data manipulation. The infrastructure must include audit management systems tracking compliance with PCI DSS and other regulatory requirements, with capabilities for documenting and tracking remediation of findings. Risk management systems must maintain asset inventories, vulnerability assessments, and threat monitoring, while supporting vendor security assessments and hardening verification. All systems must provide detailed audit trails and support regular testing of control effectiveness.	Kiteworks delivers detailed activity tracking through comprehensive system-level logs that capture all user interactions, including successful and failed logins, uploads, downloads, views, and administrative activities. These logs are exported to SIEM systems through Syslog and Splunk Universal Forwarder for advanced analysis and reporting. The platform's hardened virtual appliance ensures secure configurations through multiple security features: embedded network firewall limiting entry points, web application firewall (WAF) blocking API attacks, IP address blocking Fail2Ban system, zero-trust architecture with tiered positioning, and double encryption for data protection. Open-source library sandboxing and restricted admin access provide additional security layers. For risk management, Kiteworks aligns with NIST CSF framework and implements comprehensive DevSecOps practices. The platform provides continuous security monitoring through Enterprise subscription product focused Embedded MDR (Managed Detection and Response) and intrusion detection capabilities, supported by automated and manual penetration testing, white and black box bounty programs, and continuous vulnerability assessments. Asset classification and threat assessment are managed through content-based risk policies, while the CISO Dashboard provides compliance-specific reporting and risk analysis. The system's zero-trust assume breach architecture ensures multiple security layers protect against unauthorized access and data breaches.

Chapter 6: Business Continuity Management

This chapter establishes comprehensive business continuity and disaster recovery requirements for Qatar banks. It mandates the establishment of BCM plans aligned with ISO 22301, including emergency response procedures, incident management, and cyber crisis management. Banks must conduct regular testing through four annual drills, maintain documented recovery procedures, and establish specific protocols for cyber incidents. The requirements emphasize stakeholder communication, systematic testing, and coordinated resilience planning with vendors.

Chapter Requirements	Kiteworks Solution
Banks must implement comprehensive technical controls to support cyber crisis management. These include automated incident detection and classification systems, threat intelligence platforms integrated with local and international sources, and automated quarantine capabilities for compromised systems. The infrastructure must include real-time monitoring systems capable of detecting zero-day attacks, DDoS attempts, malware, and phishing threats, with automated response mechanisms. Systems must support coordinated testing with vendors and partners, while maintaining detailed incident tracking and response documentation.	For incident detection and response, the platform combines intrusion and anomaly detection with a product-focused Embedded MDR (Managed Detection and Response) in the Enterprise subscription that provides 24/7 monitoring and threat detection through built-in telemetry. The system's hardened virtual appliance implements multiple protection layers, including embedded network firewall, WAF, IP address blocking, and zero-trust architecture, to minimize the risk of cyberattacks. For emerging threats, Kiteworks maintains continuous security testing through comprehensive DevSecOps practices, including automated and manual penetration testing, and white and black box bounty programs. The platform supports incident containment through tiered internal services with zero-trust principles and open-source library sandboxing. All security events are tracked through comprehensive audit logs with SIEM integration, enabling detailed incident analysis and reporting. The system's multilayered approach includes collaborative testing capabilities and continuous threat intelligence updates through its MDR system.

Chapter 8: IT Operations

Comprehensive IT operational requirements for Qatar banks are outlined, covering key areas including change management, incident handling, patch management, logging, capacity planning, and access controls. It mandates structured processes for managing system changes, responding to security incidents, monitoring system performance, and controlling user access. The requirements emphasize security through detailed logging, continuous monitoring, backup management, and strict access control policies based on least privilege principles.

Chapter Requirements	Kiteworks Solution
Banks must implement comprehensive technical controls across multiple operational areas. Required systems include access control mechanisms with RBAC and multi-factor authentication, audit logging tools that track all user activities, and email security gateways with content filtering. Infrastructure must include web proxies, network monitoring systems, and backup solutions with encryption capabilities. Remote access requires secure VPN connections with endpoint protection. Change management needs separate development environments, while user activity monitoring requires automated systems for detecting unauthorized access and policy violations. All systems must maintain detailed audit trails and support incident response procedures.	The platform implements robust authentication through multiple methods including MFA, SAML SSO, and certificate-based authentication, while enforcing role-based access controls through its zero-trust architecture. For email and web security, Kiteworks provides embedded security gateways with content filtering and threat protection. The platform's hardened virtual appliance includes network and web application firewalls, IP blocking, and intrusion detection capabilities. Remote access is secured through end-to-end encryption and MFA requirements. All system activities are tracked through comprehensive audit logs with SIEM integration, while detailed compliance reporting is available through the CISO Dashboard. The platform's clustering capabilities support separate environments for development and testing, with secure replication across production and DR systems.

Chapter 9: Enterprise Security

Comprehensive enterprise security requirements for Qatar banks, covering network infrastructure, data protection, cyber threat management, and outsourcing controls, are covered here. It mandates specific security measures for network segmentation, access controls, encryption, and monitoring systems. The requirements emphasize defense-in-depth security architecture, continuous vulnerability assessment, and stringent controls for data centers and outsourced services. Special attention is given to wireless security, virtualization, and database protection.

Chapter Requirements	Kiteworks Solution
To comply with Qatar's data center and outsourcing requirements, banks must implement comprehensive technical controls across multiple areas. Data centers must be located within Qatar and equipped with physical security systems including surveillance, access control systems, and environmental monitoring for temperature, power, and fire protection. For outsourced services, secure communication channels using end-to-end encryption are required, along with monitoring systems to track vendor activities and changes. Technical controls must include media management systems for classification, tracking, and secure disposal, HSM modules for cryptographic operations, and automated systems for integrity checking of backups. All data center operations require continuous monitoring through audit logs, and vendor access must be controlled through change management systems with separate test environments.	Kiteworks supports compliance with Qatar's network and infrastructure security requirements through its comprehensive security architecture. The platform's hardened virtual appliance implements defense in-depth through multiple layers including embedded network firewall, web application firewall (WAF), and IP address blocking. For network segmentation, Kiteworks uses tiered internal services with zero-trust principles where services communicate through cryptographically secure channels. The platform maintains network security through intrusion and anomaly detection that provides continuous monitoring of suspicious activities, while comprehensive audit logs track all system and user activities in real time. Security is enhanced through open-source library sandboxing, automated and manual penetration testing, and Embedded MDR capabilities that provide 24/7 security monitoring and threat detection. All communications are protected using TLS 1.3/1.2 encryption with customer-owned keys.

Chapter 10: Business Applications

The final chapter outlines the comprehensive fraud management and business application security requirements for Qatar banks. It covers internal and external fraud controls, transaction monitoring systems, and security measures for online banking, mobile services, and payment systems. The requirements emphasize multi-layered security controls including fraud detection systems, customer authentication, PCI DSS compliance, and physical security for ATMs and POS terminals, while mandating customer awareness programs and incident reporting procedures.

Chapter Requirements	Kiteworks Solution
Banks must implement comprehensive technical controls for fraud monitoring and prevention. Required systems include real-time transaction monitoring with rule-based controls and velocity checks, coupled with payment acquiring systems. Authentication controls must include two-factor authentication, transaction passwords, and multi-channel verification for payee registration. Access management systems must enforce role-based restrictions and audit trails. Advanced analytics tools are needed to process large data volumes for fraud detection, while secure storage systems must protect sensitive card data and account information. Additionally, systems must support customer alert mechanisms including SMS notifications and dedicated communication channels for fraud reporting.	Kiteworks supports fraud monitoring requirements by securing and tracking sensitive unstructured data related to financial transactions and investigations. The platform's intrusion and anomaly detection system maintains an evolving library of patterns to monitor and detect suspicious activities around confidential financial documentation, while content-based risk policies enable dynamic rule-based controls for document access and sharing. For secure handling of fraud investigation data, Kiteworks provides comprehensive authentication methods including MFA with SMS and email-based OTP, along with role-based access controls ensuring only authorized personnel can access sensitive case files. The CISO Dashboard enables detailed activity monitoring through comprehensive audit logs that are fed to SIEM systems in real time, helping track any unauthorized access attempts to sensitive financial records. The system's single-tenant private cloud architecture and double encryption protect confidential investigation data, while detailed audit logs support forensic analysis of document access and sharing.