Kiteworks

COMPLIANCE BRIEF

Kiteworks Empowers Qatar Banks to Meet QCB Technology Risks Requirements

Comprehensive Security Features and Robust Data Protection for Sensitive Unstructured Data

The Qatar Central Bank (QCB) Technology Risks circular of 2018 establishes comprehensive cybersecurity and technology risk management requirements for banks operating in Qatar. The regulation applies to all banks in the country and covers multiple aspects of technology risk management, including cybersecurity governance, IT operations, enterprise security, business continuity, and fraud prevention. According to the circular, banks must implement robust cybersecurity frameworks, maintain dedicated information security teams, and conduct regular risk assessments and audits. Noncompliance exposes banks to various risks, including regulatory penalties, reputational damage, and potential cyberattacks that could lead to financial losses and operational disruptions. The Kiteworks Private Content Network empowers banks to share sensitive content with trusted parties at the highest levels of security, governance, and compliance while maintaining full visibility and control over their file sharing activities, helping them meet the QCB Technology Risks requirements.

Cybersecurity Within the Organization Supported With Kiteworks' ISO 27001 Certification and Robust Access Controls

Qatar's QCB Technology Risks circular mandates that banks establish a dedicated cybersecurity function with board oversight, appoint an independent CISO, and maintain a comprehensive security program. Banks must implement robust identity and access management systems, security incident monitoring capabilities, and regular system security reviews. Kiteworks helps banks meet these requirements through its ISO 27001-certified platform, which offers multiple authentication methods such as MFA, SAML 2.0 SSO, and active directory integration. The platform's intrusion and anomaly detection capabilities, coupled with SIEM-integrated audit logs, enable thorough security incident review and system configuration monitoring. Kiteworks' security architecture supports compliance through standardized log data aggregation and robust authentication controls, helping banks maintain the systematic security monitoring and access controls required by QCB regulations.

Solution Highlights

- ISO 27001-certified platform
- Intrusion and anomaly detection
- Access controls
- Zero-trust architecture
- Comprehensive audit logs
- SIEM integration

Cybersecurity in HR, Legal and Compliance, Procurement, and Risk Departments via Comprehensive Activity Tracking and Hardened Virtual Appliance

These chapters outline comprehensive cybersecurity requirements across HR, Legal/Compliance, Procurement, and Risk departments in Qatar's banking sector. Banks must implement technical controls for data protection, visitor management, access management, audit management, and risk management. Kiteworks delivers detailed activity tracking through comprehensive system-level logs that capture all user interactions, which are exported to SIEM systems for advanced analysis and reporting. The platform's hardened virtual appliance ensures secure configurations through multiple security features, including embedded network firewall, WAF, IP address blocking, and zero-trust architecture. Kiteworks aligns with the NIST CSF framework and implements comprehensive DevSecOps practices, providing continuous security monitoring, asset classification, and threat assessment through content-based risk policies and the CISO Dashboard.

Business Continuity Management With 24/7 Monitoring and Multilayered Protection to Minimize Cyber Risks

This chapter establishes comprehensive business continuity and disaster recovery requirements for Qatar banks, mandating the establishment of BCM plans aligned with ISO 22301. Banks must implement technical controls to support cyber crisis management, including automated incident detection and classification systems, threat intelligence platforms, and automated quarantine capabilities for compromised systems. Kiteworks combines Intrusion and anomaly detection with an Embedded MDR (Managed Detection and Response) in the Enterprise subscription, providing 24/7 monitoring and threat detection. The platform's hardened virtual appliance implements multiple protection layers to minimize the risk of cyberattacks, while continuous security testing through DevSecOps practices, including automated and manual penetration testing, ensures the system's resilience. Kiteworks supports incident containment through tiered internal services with zero-trust principles and open-source library sandboxing, with comprehensive audit logs enabling detailed incident analysis and reporting.

IT Operations Supported With Zero-trust Architecture and Comprehensive Audit Logs

Qatar's QCB Technology Risks circular outlines comprehensive IT operational requirements for banks, covering key areas including change management, incident handling, patch management, logging, capacity planning, and access controls. Banks must implement technical controls across multiple operational areas, such as access control mechanisms with RBAC and multi-factor authentication, audit logging tools, email security gateways, web proxies, and secure remote access. Kiteworks implements robust authentication through multiple methods, enforces role-based access controls through its zero-trust architecture, and 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, while comprehensive audit logs enable detailed compliance reporting through the CISO Dashboard. Kiteworks' clustering capabilities support separate environments for development and testing, with secure replication across production and DR systems.

Enterprise Security Supported by Defense-in-Depth Approach and Continuous Threat Monitoring to Protect Network Infrastructure

This chapter covers comprehensive enterprise security requirements for Qatar banks, including network infrastructure, data protection, cyber threat management, and outsourcing controls. Banks must implement technical controls for data centers and outsourced services, such as physical security systems, secure communication channels, media management systems, HSM modules, and automated systems for integrity checking of backups. 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, WAF, and IP address blocking. Kiteworks uses tiered internal services with zero-trust principles for network segmentation, while intrusion and anomaly detection provides continuous monitoring of suspicious activities. Security is enhanced through open-source library sandboxing, automated and manual penetration testing, and Embedded MDR capabilities, with all communications protected using TLS 1.3/1.2 encryption and customer-owned keys.

Business Applications Protected With Intrusion Detection and Content-based Risk Policies to Bolster Fraud Monitoring Efforts

The final chapter outlines comprehensive fraud management and business application security requirements for Qatar banks, covering internal and external fraud controls, transaction monitoring systems, and security measures for online banking, mobile services, and payment systems. While Kiteworks is not a credit card transaction platform, it 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 monitors and detects suspicious activities around confidential financial documentation, while content-based risk policies enable dynamic rule-based controls for document access and sharing. Kiteworks provides comprehensive authentication methods, role-based access controls, and detailed activity monitoring through the CISO Dashboard and comprehensive audit logs. 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, ensuring that sensitive unstructured data remains secure throughout its life cycle.

The Kiteworks Private Content Network offers a comprehensive solution for Qatar banks working to comply with the QCB Technology Risks circular of 2018. With its ISO 27001-certified platform, robust access controls, and advanced security features, Kiteworks enables banks to establish a strong cybersecurity posture across various departments and functions. The platform's intrusion detection, anomaly detection, and continuous monitoring capabilities help banks identify and respond to cyber threats effectively. Kiteworks' zero-trust architecture, content-based risk policies, and comprehensive audit logs ensure that sensitive unstructured data remains secure throughout its life cycle, supporting compliance with data protection and fraud monitoring requirements. By leveraging Kiteworks' powerful security features and data governance capabilities, Qatar banks are supported in meeting the stringent cybersecurity and technology risk management requirements set forth by the QCB, while safeguarding their sensitive data and maintaining operational resilience.