Kiteworks

COMPLIANCE BRIEF

Kiteworks Enables Robust FINMA Circular 2023/1 "Operational risks and resilience – banks" Regulatory Compliance

Unified Critical Data Protection and Integrated Controls Simplify Adherence to Swiss Financial Oversight Expectations

FINMA is the Swiss authority that supervises and regulates financial institutions in Switzerland. Its full name in German is "Eidgenössische Finanzmarktaufsicht," which translates to Federal Financial Market Supervisory Authority. Banks, securities dealers, financial groups, and conglomerates must ensure full compliance with FINMA's Circular 2023/1 "Operational risks and resilience – banks" to avoid significant regulatory, financial, and reputational repercussions. Noncompliance poses substantial prudential risks that could threaten an institution's stability and viability. Violations can result in enforcement actions, restrictions on activities, fines, and even loss of operating license. Given complex interlinkages, problems at one institution can rapidly spill over, disrupting financial markets. Thus, regulators prioritize safeguards like the operational resilience and continuity measures outlined in the Circular. While smaller firms have some proportional exemptions, operational risks know no size limits. All banks and securities dealers must apply the fundamentals, while global/systemic institutions and groups should expect full conformity and rigorous testing. The stakes are elevated for banks with retail and commercial lending, as operational failures stand to immediately impact customers and counterparties. But the reach of this Circular extends across banking, trading, insurance, and beyond. Kiteworks offers support in complying with this Circular. Here's how:

Operational Risk Management With Layered Security

Banks are required to categorize operational risks, assess inherent and residual risks, implement key controls and mitigation measures, conduct regular risk and control assessments, monitor losses and indicators relative to risk tolerance set by the Board, and provide risk reporting to senior management. Kiteworks' hardened virtual appliance and layered security model minimize attack surfaces to avoid operational disruptions. Its zero-trust architecture assumes breach, sandboxing components, and double encryption of data protect unstructured data. Comprehensive activity logs track administrative actions, intrusion attempts, anomalies, and user activities for each file and system component. Logs feed SIEM systems to enable quick compliance audits, security forensics, and hunting threats in progress. Granular policies control IP and data access. Authentication options include MFA and SSO to control access and is designed for least privilege. These capabilities help Swiss financial institutions implement key FINMA requirements for resilience, continuity, security, and compliance in bank systems and operations.

Solution Highlights

Granular access controls

Detailed activity logs

Zero-trust architecture

Configurable geo/IP restrictions

Third-party integration

Implement and Enforce ICT Risk Management

Institutions must implement IT governance procedures, change management processes, maintain inventories and continuity plans for ICT assets and operations, restrict development/testing environments, validate systems requirements, and establish incident response capabilities regarding significant IT failures or cyber incidents. Kiteworks logs all system and user activities for security monitoring, incident response, and audits. Its hardened virtual appliance minimizes attack surfaces with embedded firewalls, web app firewalls, and intrusion detection. Automated penetration testing and bug bounties ensure vulnerabilities are found and fixed fast. One-click cluster updates provide turnkey patching. These practices enable FINMA's expectations for financial sector ICT governance and operational resilience.

Enable Swift Reporting for Cyber Risk Management

Banks need threat assessment, data and system protection, and detection and response capabilities as per international cybersecurity standards. They must report material attacks to FINMA within 72 hours, conduct vulnerability testing and scenario exercises regularly, and analyze and remedy gaps revealed through attempts. Kiteworks is hardened through layers like embedded firewalls, web app firewalls, IP blocking, and an intrusion detection system. Sandboxing isolates software components while encryption and access controls limit data and system access. Configurable cyber threat intelligence integrates with SIEM monitoring. Together these capabilities support implementation of FINMA's expectations for identification, protection, detection, response, and recovery from cyber risks within Swiss financial institutions.

Consistent Protections for Critical Data Risk Management

Financial institutions must create a framework to classify sensitive data by criticality, restrict access through authorization systems and monitoring, select trusted service providers, create heightened safeguards for availability/integrity/confidentiality across outsourced and transmitted datasets based on data sensitivity and location risks, and report incidents breaching critical data integrity. Kiteworks' Enterprise Connect integration bridges unstructured data under centralized data governance. Policies classify sensitivity, encryption secures data, and granular permissions control access across integrated repositories like SharePoint and Dropbox. Tracking logs user activities across this unified ecosystem to produce consolidated audit trails proving compliance. The platform enables consistent critical data protections and oversight across Swiss bank systems while reducing risks from fragmented security models. Role restrictions, anomaly detection, and access controls spanning third-party systems help satisfy FINMA requirements for securing sensitive financial data and detecting unauthorized access attempts.

Centralized Cross-border Risk Management

Institutions need to thoroughly assess risks in cross-border operations, implement necessary measures to address foreign legal/regulatory exposures, ensure country-specific expertise, and exercise diligence when engaging third-party partners that provide offshore services. Kiteworks enables centralized governance over Swiss bank data shared abroad. Configurable IP and country and geographic access restrictions control cross-border data flows based on user role and content sensitivity. Legal protections apply encryption across on-premises, cloud repositories and in transit. Detailed activity logs provide audit trails spanning integrated global systems to prove compliance. Together these cross-border controls support FINMA requirements to assess offshore service risks, enforce Swiss confidentiality provisions extra-territorially, demonstrate compliance across jurisdictions, and contain exposure to foreign legal and regulatory regimes.

Kiteworks provides integrated, unstructured data security, governance, and oversight essential for FINMA regulatory compliance. Its resilience-focused architecture, encryption, access controls, and activity tracking implement operational risk, ICT, cyber, and data security expectations. The platform bridges disparate environments to enable centralized policies, integrated auditing/forensics and rapid, turnkey patching. Configurable IP, country, and systems access restrictions support Swiss confidentiality rules applied abroad. Together these unified capabilities reduce compliance costs for financial institutions by consolidating security and eliminating fragmented tools and controls, while strengthening protections for banking stability and consumer data sovereignty.