Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports UK FCA Operational Resilience Requirements With Automated Security Controls

Unified Platform for Infrastructure Mapping, Testing Documentation, and Risk Mitigation

The U.K. Financial Conduct Authority (FCA) has established new operational resilience requirements for banks, building societies, investment firms, insurers, e-money institutions, and payment service providers operating in the U.K. The rules aim to ensure firms can prevent, adapt to, respond to, recover from, and learn from operational disruptions while maintaining critical business services. Organizations had to identify important business services, set impact tolerances, and implement robust testing by March 31, 2022. They then have until March 31, 2025, to prove they can operate consistently within defined impact tolerances. The regulations require firms to map dependencies, conduct scenario testing, maintain communication strategies, and document self-assessments. Noncompliance could result in FCA enforcement actions, including potential fines and business restrictions. Kiteworks helps organizations meet these requirements through comprehensive content security, governance, and compliance capabilities that support operational resilience objectives.

Mapping Infrastructure and Communications—Comprehensive Audit Logs and Automated Threat Monitoring Drive Operational Resilience

The FCA requires firms to maintain detailed documentation of their operational infrastructure, including mapping all people, processes, technology, facilities, and information that support important business services. This mapping must enable firms to identify and address vulnerabilities. Additionally, organizations must implement internal and external communication strategies to quickly mitigate harm from operational disruptions. Kiteworks addresses these requirements through comprehensive audit logging that feeds standardized data to SIEM platforms in real time, enabling firms to document and monitor their content communications infrastructure. The platform's intrusion and anomaly detection capabilities help identify vulnerabilities using pattern recognition and tripwires. Zero-trust architecture with tiered internal services prevents unauthorized access. For communication strategies, Kiteworks provides insider and outsider threat monitoring through compliance reports that track user activities and communications. Automated notifications and file quarantine capabilities allow rapid response to contain potential disruptions and limit operational impact.

Solution Highlights

Comprehensive audit logging

SIEM integration

Zero-trust architecture

Real-time intrusion and anomaly detection

Documentation and Retention Requirements—Unified Audit Logs and Automated SIEM Integration Enable Comprehensive Compliance Records

The FCA mandates comprehensive documentation of operational resilience assessments, including records of important business services, impact tolerances, mapping approaches, testing plans, scenario testing results, and lessons learned. These records must be retained for six years and made available to regulators upon request. Kiteworks enables this documentation through unified audit logs that consolidate all system activities with consistent formatting and terminology. The platform tracks multiple activity types—from logins to file transfers to administrative actions—with detailed metadata including dates, users, IP addresses, and activity specifics. Built-in compliance summary reports cover key regulations and risk policies. For long-term retention and regulatory access, Kiteworks automatically exports logs through configurable syslog feeds to SIEM/SOAR platforms. The Splunk integration provides additional reporting capabilities that mirror native Kiteworks admin functionality, ensuring complete visibility of operational resilience measures.

Kiteworks provides financial institutions with the capabilities needed to meet FCA operational resilience requirements through its unified security platform. The solution enables comprehensive infrastructure mapping through detailed audit logging and monitoring of content communications. Built-in threat detection, zero-trust architecture, and automated controls help organizations identify and address vulnerabilities. Extensive compliance reporting and documentation features support testing requirements and lessons learned exercises. Long-term log retention with SIEM integration ensures regulatory access to required records. Automated notifications and quarantine capabilities enable rapid response to potential disruptions. By combining these security controls in a single platform, Kiteworks helps firms establish and maintain the operational resilience needed to protect critical business services and meet FCA requirements.

Kiteworks