Kiteworks

COMPLIANCE BRIEF

Kiteworks Europe AG Achieves BSI Cloud Computing Compliance Criteria Catalogue Attestation for German Regulated Industries

Meeting the Strictest Security Requirements for Finance, Healthcare, and Government Cloud Operations

The BSI Cloud Computing Compliance Criteria Catalogue (C5) establishes highly recommended and sectorally mandated security requirements for cloud service providers (CSPs) operating in Germany and serving German customers, particularly within regulated sectors including healthcare, government, and finance. Developed by Germany's Federal Office for Information Security (BSI), C5:2020 comprises 121 criteria across 17 domains that address critical security areas from identity management to incident response. Cloud service providers currently demonstrate compliance through independent Type 2 audits, with the updated C5:2025 version expected to finalize in 2026 and becoming mandatory in 2027. Failure to utilize a CSP with C5 attestation risks exclusion from regulated tenders (e.g., healthcare, public sector), loss of customer trust, reputational damage, and indirect legal/financial exposure from underlying regulations like GDPR. Kiteworks Europe AG has just secured a major compliance milestone, earning BSI C5 attestation through independent verification by HKKG GmbH on December 19, 2025, and proving the platform conquers one of Europe's most demanding cloud security frameworks.

Foundational Organizational Security

BSI C5 requires organizations to establish comprehensive Information Security Management Systems (ISMS) with clear policies, personnel controls, and asset management throughout the data life cycle. These foundational domains ensure consistent security practices, proper employee awareness of obligations, and systematic protection of organizational assets from creation through disposal. Kiteworks addresses these requirements through its comprehensive audit logging that captures all user and system activities in a single consolidated log, supporting ISMS documentation and policy enforcement. The platform's role-based access controls with eight default administrative roles enable proper separation of duties for personnel security. Asset management is achieved through automated tracking of all data movements, file versioning, and configurable retention policies that control file expiration and deletion. The system maintains detailed metadata for every file and folder, providing complete life-cycle visibility. User profiles enforce consistent security policies across the organization while the Risky Settings dashboard alerts administrators to deviations from secure defaults.

Solution Highlights

- Comprehensive audit logging
- Hardened virtual appliance architecture
- Multi-factor authentication support
- Double encryption with customer-owned keys
- Automated reporting
- DevSecOps implementation

Operational Security Controls to Support Operations and Identity and Access Management

The operational security domains of BSI C5 mandate proper system operations including vulnerability management and logging, and secure identity and access management with strong authentication for privileged users. These criteria ensure systems maintain security through capacity planning, malware protection, and controlled access to sensitive resources. Kiteworks implements these requirements through its hardened virtual appliance architecture with embedded network and web application firewalls that prevent unauthorized access. The platform provides comprehensive vulnerability management through continuous penetration testing, automated security updates, and embedded intrusion detection systems. Identity and access management capabilities include multi-factor authentication via RADIUS, PIV/CAC cards, SMS-based OTP, and time-based OTP supporting Google Authenticator and Microsoft Authenticator. Integration with LDAP, Active Directory, SAML 2.0, and certificate-based authentication enables centralized identity management. The system enforces least-privilege defaults with granular permission controls for folders and files while maintaining complete audit trails of all authentication attempts and access events.

Enable Protection of Data and Empower Customer Control Over Information

BSI C5's technical safeguards require robust cryptography for data confidentiality and integrity, secure network communications protecting information in transit, and capabilities for data portability including retrieval at contract termination and secure deletion. These domains ensure data remains protected across all states and customers retain control over their information. Kiteworks implements double encryption for data at rest using separate file-level and disk-level encryption with customer-owned keys. The platform uses TLS 1.3 and 1.2 for transit encryption with AES-256 by default. Communication security features include network segmentation for customer data traffic, DDoS protection, and tiered internal services following zero-trust principles. Data portability is ensured through comprehensive export capabilities via API and bulk download features. The platform provides secure data deletion that prevents recovery, with configurable retention periods and grace periods for deleted files. Hardware Security Module integration with SafeNet Luna and AWS KMS provides external key management options.

Support for Resilience and Rapid Response to Disruptions

Secure development practices are required following secure development life-cycle guidelines with separated environments, third-party risk management with monitoring, effective incident response with customer notifications, and business continuity planning with defined recovery objectives. These domains ensure resilience against disruptions and rapid response to security events. Kiteworks follows comprehensive DevSecOps practices incorporating OWASP methodologies, CWE cataloging, and CVSS v3 scoring throughout development. The platform maintains complete separation of development, test, and production environments with dedicated security team sign-off for releases. Third-party risk management includes automated tracking of all open-source components with CVE documentation in release notes. Security incident management features real-time SIEM integration via syslog and Splunk Universal Forwarder, with immediate alert notifications to administrators. Business continuity capabilities include high-availability clustering, automated failover configurations, one-click updates for rapid patching, and the Node Migration Wizard for infrastructure management. The system supports configurable RTO and RPO objectives through replicated data storage and comprehensive backup mechanisms.

Meet Regulatory Obligations and Maintain Customer Trust Through Transparency

BSI C5's compliance domains mandate identification of legal requirements like GDPR, transparent handling of government investigation requests with customer notification where permitted, and secure product configurations with vulnerability scanning and multi-factor authentication enforcement. These criteria ensure organizations meet regulatory obligations while maintaining customer trust through transparency. Kiteworks provides dedicated compliance reporting for GDPR, HIPAA, and CMMC 2.0 with automated control assessment and gap identification. The platform's audit log consolidates all system activities for regulatory proof, while specialized dashboards enable compliance officers to monitor adherence to specific regulations. Investigation request handling includes detailed logging of all government inquiries with automated customer notifications unless legally prohibited.

Product safety features include embedded antivirus scanning, integration with advanced threat protection systems, continuous vulnerability scanning using SAST and DAST methodologies, and mandatory MFA enforcement for administrative access. The platform undergoes annual external penetration testing with results incorporated into security improvements. SafeVIEW and SafeEDIT capabilities ensure secure data access while maintaining compliance with viewing and editing restrictions.

Kiteworks' successful BSI C5 attestation demonstrates the platform's comprehensive alignment with Germany's stringent cloud security requirements for regulated industries. The platform addresses all 17 BSI domains through an integrated security architecture that combines preventive controls, continuous monitoring, and automated compliance capabilities. By implementing defense-in-depth strategies from the hardened virtual appliance layer through application-level controls, Kiteworks ensures organizations maintain security while enabling necessary data collaboration. The platform's unified audit logging, automated compliance reporting, and centralized policy management simplify the complex task of proving continuous compliance to auditors and regulators. As organizations prepare for C5:2025's enhanced requirements, Kiteworks' existing capabilities in container management, supply chain security, and data sovereignty position customers to meet evolving standards while maintaining operational efficiency and protecting sensitive data across their entire data communications infrastructure.