Kiteworks

COMPLIANCE BRIEF

ECC-1:2018 and Kiteworks: Enhancing Cybersecurity With Robust Event Logs and Monitoring Management

Achieving Compliance, Visibility, and Control Through Unified Audit Logs, Trusted Event Tracking, and SIEM Integration

The Essential Cybersecurity Controls (ECC) are a set of mandatory controls developed by the National Cybersecurity Authority (NCA) in Saudi Arabia as part of the Vision 2030 initiative. The ECC consists of 114 core controls divided into five main components, including cybersecurity governance, defense, resilience, third-party and cloud computing cybersecurity, and industrial control systems cybersecurity. These controls aim to ensure the confidentiality, integrity, and availability of information and technology assets. They are applicable to government organizations and private sector entities operating critical infrastructures, and are encouraged for other organizations. Compliance with the ECC is assessed through self-assessments, compliance tools, and audits. Organizations must implement measures to continuously comply with the ECC. The applicability of specific controls depends on the organization's business and use of technologies such as cloud computing and industrial control systems. Kiteworks can help government organizations in the implementation of technical measures to fulfill the ECC in the different domains and subdomains. Here's how:

Cybersecurity Defense

Kiteworks is a vital solution for supporting cybersecurity and defense efforts, where strict adherence to cybersecurity requirements is crucial. Kiteworks steps in to assist organizations in meeting these stringent standards by providing secure file sharing and content communication solutions. Through its state-of-the-art features and capabilities, Kiteworks enables organizations to effectively manage highly sensitive data while complying with the rigorous Essential Cybersecurity Controls. By offering secure file sharing, real-time monitoring, and robust security features, Kiteworks helps defense organizations bolster their cybersecurity defenses and ensure compliance with regulatory mandates.

Solution Highlights


Anomaly detection and real-time monitoring


Comprehensive audit logging and reporting


Role-based access control


Content and user-based policy enforcement


Multi-factor authentication


Integration with security information and event management (SIEM) systems


Comprehensive mobile security


Secure data storage and backup


Email protection with policy control

Controls	Objective	Kiteworks Solution
2-2	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks	Kiteworks offers various authentication and authorization methods to ensure secure access to its system. It supports RADIUS 2FA/MFA, native OTP-based 2FA, and OAuth for multi-factor authentication. Additionally, it provides enterprise integrations with LDAP/AD, SSO/2FA/MFA, and authenticators such as Google, Microsoft, and Authy. Kiteworks also employs role-based policies, access controls, and configurable administrator roles to maintain least privileged access and ensure that users only have access to the resources they need.
2-3	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks	Kiteworks provides robust malware and virus protection with automatic DLP scans for file downloads and automatic AV and ATP scans for file uploads. It ensures system security and mitigates potential threats. Data is securely stored with encryption in transit and at rest. Users retain ownership of encryption keys for enhanced security. Kiteworks integrates with CMS for secure software patching and upgrades, keeping the system up to date and safeguarded against known vulnerabilities.
2-4	To ensure the protection of the organization's email service from cyber risks	Kiteworks ensures secure and protected email communications, safeguarding sensitive data. It provides secure email within the Kiteworks Private Content Network, enabling privacy, compliance, and trust with stakeholders. Kiteworks secure email, along with the Microsoft Outlook plugin, allows private emails with top-level security and compliance through encryption, policy-based rules, access controls, and auditing. The Kiteworks Email Protection Gateway automates email protection with policy-based, end-to-end encryption, shielding content from cloud providers and malware attacks. Encryption options include S/MIME, OpenPGP, TLS 1.2, and AES-256. Granular controls, automation, and governance features ensure ease of use and protection for sensitive information.
2-5	To ensure the protection of the organization's network from cyber risks	Kiteworks allows administrators to set granular, scalable administrative policies and strict access controls to manage and restrict network services, protocols, and ports. This ensures that only authorized users have access to specific services and data, enhancing the overall security of the platform. Additionally, Kiteworks can be integrated with existing security infrastructure, such as LDAP, SSO, and SIEM, to further strengthen the security posture and provide a seamless experience for users while maintaining a high level of control over network services, protocols, and ports.

Controls	Objective	Kiteworks Solution
2-6	To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the organization's information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy	The Kiteworks mobile app ensures robust security for sensitive data on mobile devices. It offers a secure container with AES-256 encryption and remote wipe functionality. The app establishes an encrypted HTTPS/TLS connection to the Kiteworks server. Multi-factor authentication methods like RADIUS 2FA, native OTP-based 2FA, and OAuth are supported. Administrators can whitelist helper applications to enhance platform security. The Express Secure Camera feature enables secure photo capture, automatic upload to Kiteworks, and segregation within the app's secure container, bypassing the device's camera roll. Kiteworks provides comprehensive mobile security features for data protection.
2-7	To ensure the confidentiality, integrity, and availability of the organization's data and information as per organizational policies and procedures, and related laws and regulations	Kiteworks ensures data and information protection while maintaining ownership for organizations. Key features include granular access controls, allowing administrators to set role-based permissions. A built-in audit log provides visibility into data access and actions taken. Compliance reporting capabilities help demonstrate adherence to regulations. Secure storage with encryption ensures authorized access. Kiteworks integrates with existing security infrastructure like LDAP, SSO, and SIEM, further strengthening data ownership and control. With these features, Kiteworks empowers organizations to securely share and collaborate while maintaining ownership and control over their valuable data.
2-8	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations	Kiteworks prioritizes data security through robust cryptographic measures. Key aspects include encryption in transit using HTTPS/TLS, safeguarding data during transmission. Data at rest is encrypted with AES-256-bit encryption, ensuring high-level protection. Kiteworks holds FIPS 140-2 compliance certification, meeting stringent U.S. government security standards for cryptographic modules. Additionally, Kiteworks has implemented FIPS 140-3 encryption libraries, pending NIST validation, to further enhance platform security. These cryptography measures guarantee that sensitive data remains secure from unauthorized access, establishing a trusted environment for organizations to store, share, and collaborate on their valuable content.

Controls	Objective	Kiteworks Solution
2-9	To ensure the protection of the organization's data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations	Kiteworks brings significant value to backup and recovery management, ensuring uninterrupted workflows and safeguarding critical data. Key features include multiple primary satellite servers, offering high availability and scalability. Automatic backups of primary servers are restored to secondary servers for quick data recovery in the event of primary server failure. Email notifications alert administrators of server issues, facilitating seamless switching to backup servers. On-demand database backups provide flexibility, separate from software updates. Kiteworks also enhances reliability and flexibility of updates by separating background processes. These backup and recovery management capabilities secure data and enable efficient restoration, ensuring continuous operations and data protection.
2-10	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyberattacks against the organization	Kiteworks delivers significant value through its robust vulnerability management practices, ensuring a secure environment for customers. Key aspects include regular vulnerability scanning to proactively identify and address security risks. Timely patches and updates are released to address vulnerabilities and enhance platform security. Kiteworks offers different deployment options with varying levels of patch management responsibility, enabling customers to choose the approach that best suits their needs. Whether deployed on-premises, hosted by Kiteworks, or with premium support, Kiteworks ensures a secure environment through comprehensive vulnerability management. This commitment protects sensitive data and safeguards workflows, instilling confidence in the platform's security posture.
2-11	To assess and evaluate the efficiency of the organization's cybersecurity defense capabilities through simulated cyberattacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber breach	Kiteworks provides significant value to organizations through its robust approach to penetration testing. Key aspects include state-of-the-art tests to identify and address vulnerabilities in the platform, ensuring adherence to security best practices. Penetration tests specifically target internet-facing vulnerabilities, safeguarding against potential external attacks. Additionally, onsite tests evaluate vulnerabilities within Kiteworks' corporate network infrastructure, enhancing overall security. Regular testing is conducted to maintain a high level of security and promptly address emerging vulnerabilities. By prioritizing penetration testing, Kiteworks showcases its commitment to maintaining a secure environment, protecting customer data, and fortifying workflows against potential threats.

Controls	Objective	Kiteworks Solution
2-12	To ensure timely collection, analysis, and monitoring of cybersecurity events for early detection of potential cyberattacks in order to prevent or minimize the negative impacts on the organization's operations	Kiteworks delivers valuable support for cybersecurity event logs and monitoring management. Key aspects include unified and standardized audit logs that consolidate activities across communication channels and system services. The system generates trusted audit logs in human-readable formats, facilitating administrative reporting, compliance audits, and end-user tracking of views, downloads, uploads, and edits. Export functionality allows logs to be integrated with SIEM systems like IBM QRadar® or FireEye Helix®. End-users can track email and file activities, while comprehensive and immutable audit logs provide a reliable record for threat identification, remediation, and forensic analysis. With these features, Kiteworks empowers organizations to maintain visibility, control, compliance, and a secure environment for their data and operations.

Cybersecurity Governance

Kiteworks is a comprehensive solution that assists organizations in meeting strict compliance requirements, including the EU's NIS 2 Directive and ISO standards, while maintaining strong cybersecurity measures. The Kiteworks platform offers advanced features and capabilities for secure data management. One of the ways Kiteworks supports cybersecurity governance is through the implementation of incident notification and record-keeping requirements. The platform maintains detailed logs and records of data access, transfers, and user activities, facilitating compliance with incident reporting obligations. Additionally, Kiteworks enables organizations to establish opt-in mechanisms, consent forms, and procedures for data collection, ensuring compliance with consent regulations and safeguarding personal information.

Cybersecurity Resilience

Kiteworks plays a crucial role in supporting cybersecurity and defense efforts by providing secure file sharing and content communication solutions for organizations. It enables organizations to maintain robust cybersecurity measures and adhere to strict compliance requirements while also ensuring business continuity. By offering state-of-the-art features and capabilities, Kiteworks helps organizations in the defense sector bolster their cybersecurity defenses and ensure compliance with regulatory mandates. Additionally, Kiteworks provides a secure and reliable platform for organizations to manage, share, and store sensitive data, contributing to business continuity. With secure data storage, real-time monitoring, and granular access controls, Kiteworks ensures that organizations can continue their operations without interruption, even in the face of potential threats or disruptions. Kiteworks not only safeguards sensitive data but also facilitates uninterrupted business operations, delivering value in terms of both cybersecurity and business continuity.

Third-party and Cloud Computing Cybersecurity

Kiteworks offers a flexible platform that supports various deployment options tailored to specific requirements, including on-premises, hybrid, hosted, and private cloud options. This flexibility allows organizations to find the perfect balance between privacy, compliance, and scalability. By leveraging Kiteworks' deployment options, organizations can confidently meet contract obligations while minimizing security risks and reducing maintenance costs. The platform's ability to address privacy, compliance, and scalability needs effectively ensures that organizations can maintain a secure environment while optimizing their resource utilization and operational efficiency.

ICS Cybersecurity

Kiteworks, a secure content communication platform, can enhance industrial control systems (ICS) cybersecurity by providing a secure way to manage, share, and store sensitive ICS-related data. Kiteworks can support organizations by offering secure data storage and sharing options, granular access controls, real-time monitoring, and incident response capabilities. Additionally, Kiteworks helps organizations maintain compliance with industry standards and regulations such as NIST. ICS cybersecurity requires a comprehensive approach, and Kiteworks can be a part of the overall strategy by providing secure content communication and data management.

In the realm of cybersecurity, compliance, visibility, and control are paramount. Kiteworks, a leading secure content communication platform, aligns with ECC-1:2018 by providing comprehensive event logs and monitoring management solutions. Kiteworks offers unified audit logs that consolidate activities across communication channels, facilitating analysis and compliance reporting. Trusted event tracking enables organizations to track file access, downloads, uploads, and edits, ensuring accountability and adherence to ECC-1:2018 requirements. Kiteworks supports SIEM integration, allowing seamless integration with security information and event management systems for efficient monitoring and early detection of potential cyberattacks. By leveraging Kiteworks' robust event logs and monitoring capabilities, organizations can bolster their cybersecurity defenses, maintain compliance, and safeguard their critical data and operations.