Kiteworks

Whitepaper

Mastering NIS-2, DORA and other regulations - Setting Up a Successful Compliance Strategy

Introduction

IT and security professionals face the dual challenge of enabling seamless, cross-platform collaboration while ensuring the integrity and confidentiality of corporate data. In addition, cyber threats are becoming increasingly complex. In 2023 alone, Germany's Federal Criminal Police Office (BKA) recorded a significant increase in the number and quality of cybercrime cases. According to BITKOM (German IT and telecom industry association), the financial damage caused by cybercrime will total 205.9 billion euros.

Response to Cyber Threats in Europe

These alarming figures highlight the urgent need for a common standard to strengthen IT security and improve protection against cyber attacks. In response, the European Union has introduced several new regulations as part of its „Digital Decade" to ensure that companies and institutions are better equipped to deal with the growing cyber threat. Key new regulations include:

NIS-2 (Network and Information Security Directive): This Directive aims to strengthen cybersecurity in the EU by establishing enhanced security measures and reporting obligations for operators of essential and critical services and digital service providers. It ensures that EU Member States take appropriate security measures and report security incidents.

DORA (Digital Operational Resilience Act): Designed specifically for the financial sector, the regulation aims to ensure that firms in the sector have the necessary digital resilience. This includes the ability to defend against cyber attacks and maintain business continuity even in the event of serious IT disruptions.

Cyber Resilience Act: This legislation aims to harmonize and improve the safety requirements for products with digital elements. This significant piece of EU legislation seeks to establish harmonized cybersecurity requirements for digital products throughout their lifecycle, aiming to enhance the overall cybersecurity resilience of hardware and software placed on the EU market.

The new regulations pose significant challenges for organizations, particularly due to the shortage of skilled workers and limited IT resources. Non-compliance could result in significant penalties, including fines and legal sanctions, as well as reputational damage and increased vulnerability to cyber attacks, which could lead to data loss and financial losses.

To effectively meet business and regulatory compliance requirements, it is crucial to adopt a comprehensive and integrated approach.

Compliance is a matter of concern for companies of all sizes and requires the time and acceptance of the entire workforce. A well-coordinated compliance strategy that is tailored to the needs of users is essential for

Principles of a Successful Compliance Strategy

The implementation of a compliance strategy is not a one-time occurrence; it is a continuous process that must be centrally managed and constantly adapted. It requires a commitment of time and the active involvement of all employees.

A successful compliance strategy can be achieved by jointly focusing on three central principles: **Protect, Track & Control**.

These approaches enable the protection of sensitive data, the transparent tracking of data flows, and the implementation of comprehensive controls to establish a sustainable and effective compliance culture within the company.

One of the most significant challenges is the implementation of these best practice principles. In the past, a multitude of communication tools and systems have been employed to facilitate the exchange of sensitive content within an organization. This has often resulted in the emergence of isolated, standalone solutions and shadow IT, which has made it challenging to implement consistent security measures and track content.

However, with new regulations and reporting requirements, it is now necessary to demonstrate all security measures in place and demonstrate an effective IT security strategy to the relevant authorities. Many organizations are now required to implement appropriate governance measures to ensure the integrity and security of data and provide a secure working environment for all employees.

PROTECT

It is imperative that sensitive data be safeguarded from unauthorized access, data theft, or misuse. This necessitates the implementation of robust security measures, including encryption, firewalls, and security protocols.

TRACK

It is vital to implement processes that monitor the transfer of sensitive data within the company‘s internal systems and with third-party providers. By documenting data flows, for instance in audit logs, potential security gaps can be identified at an early stage, allowing informed decisions to be made on how to deal with potential security risks.

CONTROL

By implementing comprehensive control mechanisms, it is possible to ensure full data control over sensitive data both in transit and at rest.

Foundations of a Robust Compliance Strategy

A proven approach to improving compliance is to **centralize and unify communications systems**. Working with a strong IT partner and implementing a Private Content Network (PCN) as a central repository creates a protected work environment. In this environment, sensitive files can be securely stored, shared and collaborated on without compromising data security. This governance measure allows you to embed a successful compliance strategy into your own organization.

There are three key building blocks that can be provided alongside your IT partner:

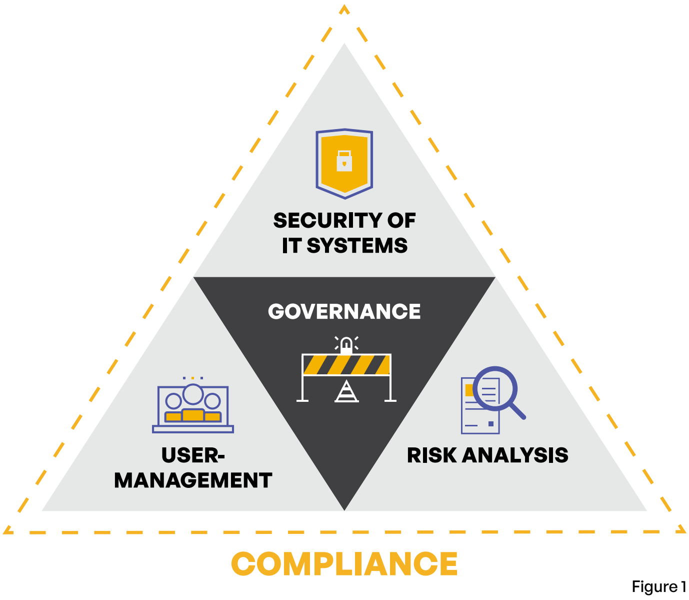

Figure 1

Security of IT Systems

The Security of IT Systems module includes all measures and processes that help protect IT infrastructures from unauthorized access, data loss, and cyber-attacks. Considering the first principle „PROTECT“, this includes the implementation of robust security protocols, encryption mechanisms and access controls. The goal is to ensure the integrity, confidentiality, and availability of data.

A Private Content Network with its advanced security features can significantly support and accelerate the security process. By providing features such as double encryption, multi-layered protection mechanisms (e.g., proactive deletion of inactive data), and a zero-trust architecture, a PCN helps to comprehensively protect IT systems, defend threats, ensure the confidentiality of data, and enable the secure exchange of information (e.g., via share links).

Risk analysis

The Risk Analysis module involves the systematic identification, assessment, and prioritization of risks that could affect an organization‘s IT infrastructure. Considering the second principle, TRACK, risk analysis involves the continuous monitoring and assessment of threats and vulnerabilities. The goal is to take appropriate risk mitigation measures and understand the likelihood of the potential impact of security incidents.

A Private Content Network, with its advanced risk tracking and mitigation capabilities, can help identify security vulnerabilities faster and address them before they occur. These features include customizable reports that enable detailed risk analysis and identification of specific threats. Comprehensive audit logs help quickly identify security vulnerabilities and enable detailed tracking of activities and changes within IT systems.

By integrating security data from across the IT environment into a SIEM system, security events and incidents can be centrally monitored and configured to automatically alert you to compliance violations or security risks. This helps you detect threats and attacks, prioritize security risks, and remediate vulnerabilities in a timely manner.

Figure 1 - Building blocks of a successful compliance strategy

User Management

The User Management module includes all measures and processes that contribute to the administration and control of user accounts and access rights within an IT infrastructure. Considering the third principle „CONTROL", comprehensive user management includes the monitoring and administration of access rights as well as regular security training for all employees.

A Private Content Network prevents unauthorized access to data by using secure authentication methods at login to ensure that only authorized users have access to sensitive data and systems, and that (stolen) login credentials - e.g. after a phishing attack - cannot be misused. Role-based user rights assignment can further restrict access to sensitive data, ensuring that access rights are assigned based on the user's specific roles and responsibilities (read/write/delete).

A Private Content Network also provides a protected work environment and a secure storage location for sensitive data that can be accessed in real time from anywhere. This greatly increases the flexibility and efficiency of users, making it more likely to become a part of everyday work life.

Regular training and communication updates ensure user awareness of security issues and adherence to compliance policies.

Mastering Compliance - How to Create a Lasting Culture of Compliance

Combining the three basic building blocks Security of IT Systems, Risk Analysis, and User Management provides the foundation for a robust compliance strategy. With the support of a strong IT partner, an organization's IT department can be relieved, and the skills shortage can be effectively addressed. A Private Content Network can significantly improve the security and efficiency of IT infrastructures over the long term, supporting compliance with legal and regulatory requirements.

However, it is not only the interaction of these factors that leads to a sustainable and successful compliance culture. When planning strategies, don't forget to talk to each other. The focus is on taking the right steps and using the right features to ensure greater security. But the only way to effectively embed compliance as part of the corporate culture is through two-way communication. Be present in different departments and talk about compliance and all related topics (such as preventing shadow IT or reducing duplication).

To ensure the long-term success of your compliance culture, you should periodically review it. Analyze the entire process - how policies and procedures have been communicated and integrated into your organization - and objectively assess their timeliness and effectiveness. Ongoing communication and commitment from all stakeholders, especially managers, are critical to embedding a lasting culture of compliance within the organization. Managers should act as role models and actively contribute to maintaining and promoting compliance to reinforce the importance and value of these measures throughout the organization.

Kiteworks

About Kiteworks

Kiteworks' Private Content Network helps you meet many compliance requirements and enhance your IT security. Our ISO 27001, 27017 and 27018 certifications demonstrate a high level of data security and provide a solid foundation for full control and integrity of your sensitive corporate data. As a strong partner, Kiteworks can help you meet compliance requirements by helping you implement appropriate security mechanisms (PROTECT), meet regulatory reporting requirements by quickly tracking and identifying security vulnerabilities (TRACK), and control data by implementing appropriate cyber hygiene controls within your organization (CONTROL).

Check it out for yourself and try Kiteworks at no charge or get in touch with us for a non-binding consultation.

Try our free demo now!

Try Now

Learn more about Compliance.

Learn More

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.

June 2024

www.kiteworks.com