Compliance and Data Security Audits Identify Risks, Protect Business Data

Digital transformation has opened the door for unprecedented innovation and growth. Data informs marketing and development while improving customer service and streamlining processes. At the same time, privacy regulations and increasing cyber threats add complexity. Compliance and data security audits can help organizations navigate the environment.

Though distinct from one another, regulatory compliance and security prove equally essential for business success. When organizations understand how compliance and security differ, as well as how they complement one another, they can significantly reduce risk. Audits form a key part of that process.

Regulatory Compliance

From the perspective of IT security, compliance refers to ensuring that an organization meets applicable data security and privacy standards. These can include legislation such as GDPR, as well as industry-specific standards like HIPAA and any contractual obligations.

Regulatory compliance often includes a significant security component. For instance, HIPAA regulations require organizations to demonstrate safeguards that protect against unauthorized access to PHI. Likewise, PCI-DSS requirements include mandates for firewalls and encryption to protect cardholder data.

However, organizations should not assume that achieving compliance means ensuring security. The goal of a compliance audit involves satisfying regulatory requirements to avoid fines and maintain the ability to operate.

Data Security

Data security, on the other hand, involves maintaining data confidentiality and integrity while ensuring data availability (the CIA triad). This includes addressing technical, administrative, and physical controls.

The goals of data security include keeping business data and infrastructure safe from attack and minimizing damage when attacks do occur. Because bad actors continually develop more sophisticated tools and methods, these goals require constant vigilance.

In short, while compliance aims to satisfy legal and regulatory demands, security strives to protect vital assets within a constantly evolving threat landscape. Consequently, because regulations typically lag emerging threats, an organization can achieve compliance and still remain unsecure.

Benefits of Conducting Regular Compliance and Data Security Audits

Compliance audits and security audits serve important functions. In addition to holding organizations accountable, they highlight risks, a critical first step in developing effective security programs. An audit may be imposed by a third party. Additionally, a proactive company will conduct regular compliance and security risk assessments as part of an overall strategy.

While companies can focus on simply passing the annual audit, successful organizations move beyond checkbox security. These organizations use audits as an opportunity to illuminate areas for improvement and involve stakeholders from across the company. When approached from this perspective, audits deliver several key benefits.

First and foremost, an audit forms an essential role in ensuring the security of sensitive data. In addition to pointing out vulnerabilities, it ensures the enforcement of data security policies and raises awareness about security best practices. Regular audits provide a measuring tool to determine the effectiveness of security training programs.

Audits also help the company avoid heavy penalties for non-compliance. Even if a breach does occur, the audit documentation may help to reduce any penalties levied. And demonstrating a commitment to compliance and security improves the company's reputation in the marketplace.

Compliance and Security: Complementary Efforts

While compliance and security differ in approach and purpose, they share similar goals relating to managing risk and protecting sensitive data. Working in concert, compliance and security efforts serve to strengthen the organization.

For instance, although compliance does not guarantee data security, it does offer a useful framework from which to expand. Likewise, strong security controls do more than protect data from unauthorized access. They also help avoid damage to the company reputation caused by non-compliance.

The compliance and security experts at Messaging Architects can help, starting with a security audit and ongoing compliance monitoring. We deliver the tools you need to gain visibility into your data, automate compliance and optimize risk controls to keep data secure.