Navigating the Labyrinth: Top 6 Compliance Mistakes Organizations Make

In today's complex regulatory landscape, staying compliant feels like negotiating a maze. One wrong turn can lead to hefty fines, reputational damage, and legal repercussions. However, when companies understand common compliance mistakes and take proactive steps, compliance becomes an organic part of doing business.

1. Ignorance is Not Bliss: Failing to Keep Up with Regulations

GDPR took effect in 2018, initiating a cascade of regulations across the globe. New privacy laws and industry regulations appear on the scene every year, and governing bodies regularly make adjustments. If organizations neglect to stay on top of regulatory changes, they may mistakenly assume they are compliant. But pleading ignorance will not help them avoid penalties.

Solution:

- Regularly monitor updates from governments and other relevant regulatory bodies specific to your industry.
- Conduct regular compliance audits.
- Collaborate with legal experts or compliance professionals who specialize in demystifying regulations.
- Attend industry conferences or webinars where experts discuss changes.

2. Unlocked Doors: Losing Focus on Cyber Security

Organizations, particularly in highly regulated industries such as healthcare, have a legal and ethical responsibility to protect sensitive data from unauthorized access. Most data privacy laws and other regulations include strict security mandates. And regulatory violations from data breaches can result in both hefty fines and lost customers.

Solution:

- Conduct cyber security assessments to highlight vulnerabilities and measure effectiveness of security measures.
- Promptly apply security patches to software and firmware.
- Implement network segmentation, dividing the network into smaller segments based on risk levels or business needs.
- Apply zero trust architecture, in which every access request is subject to digital verification.
- Strengthen protection with multi-factor authentication.

3. Wild Data: Underestimating the Power of Information Governance

Legislation such as HIPAA requires retention of certain types of data. On the other hand, some privacy regulations grant individuals the right to access, correct, or request deletion of their data. To comply with these regulations, organizations must know where that information lives, how the company uses it, and who has access to it. Enter information governance.

Solution:

Robust information governance provides visibility into data throughout the organization. It also streamlines data classification, allowing data teams to apply policies for retention, data sharing, and encryption according to data type. Ongoing compliance and security monitoring helps to reduce the risk of non-compliance.

4. The Human Factor: Overlooking Employee Training and Awareness

Many compliance violations arise from human error. If individuals do not understand the rules and regulations that apply to their roles, they may unwittingly invite a data breach. For instance, employees may share sensitive information inappropriately or click a malicious link in a phishing email.

Solution:

Compliance training and security awareness training are essential, but they need to engage the learner to have the desired effect. Avoid lengthy lectures. Instead, employ various methods to engage different types of learners. Use real-world scenarios and target training to specific roles. Finally, regularly update training to reflect changing regulations and industry standards.

5. Partner Problems: Forgetting to Review Vendor Contracts

Organizations may not realize that regulations such as CCPA and GDPR also apply to the actions of third parties. For example, in 2021 a billing company that contracted with the California Department of Motor Vehicles suffered a ransomware attack. Because the attack exposed vehicle and driver records, the DMV was held liable for the data breach.

Solution:

Carefully monitor contracts with service providers and other third parties. Look for stipulations requiring vendors to maintain reasonable security practices regarding sensitive data. Also know and monitor all points through which third parties access company networks and data.

6. Unused Toolbox: Neglecting to Leverage Compliance Technology

Yesterday's cyber security tools cannot keep up with today's AI-powered cyber threats. Likewise, humans alone cannot feasibly track, manage, and analyze massive amounts of data to maintain compliance.

Solution:

Invest in carefully-chosen compliance technology to automate key tasks such as data collection and classification. AI-enhanced tools provide the ability to manage data at scale. They can also ease the process of analyzing data privacy laws and industry regulations to identify necessary changes to internal processes. Compliance monitoring also plays a critical role.

Steer Clear of Common Compliance Mistakes

Achieving and maintaining compliance requires an investment of both budget and resources. However, the true costs of non-compliance can devastate the company's bottom line. And in today's business environment, organizations cannot afford to take the risk.

Partnering with compliance experts Messaging Architects will help ease the compliance burden. Leveraging intelligent compliance solutions and enterprise-grade cyber security, we provide the tools and expertise to keep sensitive data secure and compliant.