Checkbox Information Governance vs Effective Data Governance

For many organizations, the concept of information governance is intertwined with regulatory compliance. For instance, any organization that processes, stores, or transmits credit card data must demonstrate PCI compliance. However, when companies stop at checkbox information governance, they leave themselves at risk and never unlock the true power of their data assets.

Most organizations publicly pronounce a commitment to compliance and data security. But underneath the hood, the story often looks a little different. For instance, a business may put policies and tools in place for the annual compliance audit and then gradually forget about them as the months go on.

Even when organizations carefully comply with regulations, that compliance can deliver a false sense of security. On paper, the regulations sound comprehensive, even overwhelmingly so. However, no regulation will account for every situation, and legal compliance does not mean that data remains secure and effectively managed.

Instead of focusing on a compliance checklist, organizations need to build information governance into the company culture. When data privacy and security permeate everyday processes, breaches happen less often, and compliance becomes much easier.

Start with a Good Foundation

To move beyond checkbox information governance, organizations need to build information governance into the corporate culture. This means securing executive sponsorship from the beginning and involving key stakeholders from all affected areas. While tools play an important role, the success of an information governance strategy ultimately depends on personnel.

With a compliance team in place, conduct an assessment of the data landscape. This includes understanding data flow within the organization. It also involves an inventory of data policies, vendor relationships, connectivity and other factors that affect data security.

Understanding the applicable regulations will help as the organization proceeds to identify and prioritize risks. Compliance checklists can serve as starting points to help pinpoint vulnerabilities, but risk assessments should move beyond legal compliance.

For instance, instead of simply verifying the existence of security and compliance tools, test the tools. Make sure that logs actually capture the desired information. Test backups regularly. And conduct penetration testing to make sure security controls function correctly.

Automation Eases the Pain

Many businesses start information governance with good intentions, only to get bogged down by the work involved. Automating routine tasks simplifies the process while reducing the risk of errors. Good candidates for automation include data lineage and metadata management. Additionally, machine learning can play a vital role in tightening cybersecurity.

Among the other automated tasks, be sure to include ongoing compliance monitoring. Monitoring works behind the scenes to scan digital content, analyze data access and pave the way for proactive risk management.

Choose Information Governance Tools Wisely

Information governance done right involves tapping into a variety of technology resources. But not all tools deliver the same quality results. Take time to research the options available and choose tools that meet your specific needs.

For instance, Microsoft 365 Business includes an advanced eDiscovery solution. The solution delivers useful features and functionality. However, it requires users to index data and add the data to a review set before performing any eDiscovery actions. In contrast, eGovernance Cloud requires no re-indexing, allowing auditors to get results almost immediately.

Partner with Experts and Leave Checkbox Information Governance Behind

The experts at Messaging Architects bring both the tools and the deep knowledge needed to move beyond checkbox information governance. They can help you conduct risk assessments and ongoing compliance monitoring. And they will guide you through designing and implementing a comprehensive strategy to protect and optimize information assets.