Effective Information Governance Strategy Drives Data Value and Supports Business Goals

Information governance involves locating and managing information wherever it lives throughout the organization. This includes managing the data lifecycle, providing for data security, and maintaining regulatory compliance. An effective information governance strategy helps organizations achieve strategic goals while reducing risk.

However, implementing effective information governance requires careful planning and coordination. And it takes time. Organizations should start with a comprehensive data audit to inform next steps. Leveraging information governance consulting services will streamline the process.

Assess Your Current State and Future Data Goals

To begin with, the organization must learn what data it has and where it lives. An initial data audit will develop a picture of data across the enterprise. The audit includes components such as:

- Data mapping – The organization must identify where data lives and how it is stored. This will include understanding information infrastructure elements such as document libraries. It will encompass all storage locations, whether on premises or in the cloud. And it will involve identifying sensitive data.

- Determining data quality – Duplicates, outdated information, and data silos all affect the quality of data. Likewise, access issues affect the usefulness of data. If the right people cannot find and access the information they need quickly and securely, the data holds little value.
- Assessing data processes and policies – Determine what information policies exist and whether they are enforced. These include policies for accessing and sharing data as well as policies for retaining and destroying information.
- Evaluating information security – A cyber security assessment reviews the policies and security controls governing information storage, movement, and access. And it evaluates existing security measures against regulatory requirements, industry standards and business needs.

With an understanding of the current state of information, the organization can define its vision and goals for information governance, aligning those goals with business needs.

Locate and Classify Data

Data classification proves foundational to good information governance. Sensitive and important data may be hidden in documents, meeting minutes, emails, chats and more. Labeling sensitive data allows data stewards to track that data and apply essential protections such as encryption and sharing restrictions.

Manually locating and tagging data proves difficult if not impossible at scale. But AI-powered tools automate the process of finding and classifying data wherever it lives. Properly classified data simplifies regulatory compliance and eases the eDiscovery process.

Define and Implement Data Lifecycle Policies

Data classification plays a key role in enforcing data retention and destruction policies. Regulations such as PCI DSS and HIPAA include strict rules around the minimum amount of time to retain certain types of information. On the other hand, information retained too long can become a liability.

Automating retention policies according to data type gives the organization a defensible way to maintain regulatory compliance. Because regulations and business priorities evolve over time, data stewards should regularly review and update retention policies.

Ensure Compliance Management

To address mandates from a wide variety of regulations, an effective information governance strategy should include regular compliance monitoring. eGovernance monitoring tools deliver visibility into sensitive data from a single console. Content alerts and reports allow for proactive remediation. And monitoring provides proof of policy demanded by many regulations.

Build Comprehensive Data Security

Data security works hand in hand with compliance monitoring as an essential element of information governance. While regulatory compliance mandates reasonable security precautions, organizations must move beyond checkbox compliance to protect against data breaches.

A risk assessment will highlight vulnerabilities and provide a basis for security planning. Security strategies must include ensuring proper access management. Endpoint protection, encryption, data backups, and multifactor authentication prove critical, as well. And organizations must address supply chain security and provide regular security awareness training for all staff.

Adapt Information Governance Strategy to Business Needs

Company structure, business priorities and specific industry requirements all play a role in information governance. Consequently, the optimal strategy will look different from one company to another. In every organization, however, effective information governance requires engagement of stakeholders and users throughout the organization.

eGovernance delivers a cloud-based information governance solution. Our consultants will work with your organization to design and implement an information governance strategy customized to your specific business needs.