Messaging Architects

Enterprise Information Governance Next Steps to Drive Data Value

Most organizations have expansive caches of data. However, without effective enterprise information governance strategies, they may fail to tap into the full extent of their data value. Worse, mismanaged data may actually pose significant risk to the company.

For instance, in a business environment tightly governed by rapidly evolving privacy regulations, poorly governed data can result in stiff penalties and damaged reputation. Additionally, business strategies based on redundant, incomplete, or faulty data will generate poor outcomes. And haphazard data management increases the risk of a security breach.

On the other hand, when organizations build a culture of effective information governance, they improve efficiency and productivity. They power innovation, confidently build sound business strategy, and reduce cyber risk. And they gain a competitive edge with the ability to adapt quickly to regulatory and market changes.

Implementing an effective information governance program takes substantial time and effort. But tackling the challenge step by step will make it manageable. When choosing your organization's next steps, consider focusing on one of the information governance success criteria described below.

Classify Sensitive Data for Effective Management

Sensitive and essential data hides throughout the organization in Microsoft Office documents, emails, meeting transcripts, chats and more. Make it a priority to find and classify sensitive data. While manual data classification proves practically impossible to manage at scale, AI-powered tools can automatically find and tag data wherever it resides.

Data classification forms the foundation of any good information governance strategy. In addition to making data visible and retrievable, classification allows data stewards to manage both data lifecycle and data security. And it aids regulatory compliance and eDiscovery.

Ensure Compliance and Improve Data Quality with Retention Policies

In fact, data classification plays a key role in retention and destruction policies. Regulations such as HIPAA and other industry standards prescribe a minimum amount of time to retain certain types of data. On the other hand, information can prove a liability if kept too long.

Automated retention policies, tied to data type, provide organizations with a defensible way to achieve compliance while removing obsolete data. Keep in mind that ePolicies should be reviewed regularly to ensure that they support evolving regulatory requirements and business priorities.

Tailor Cyber Security Strategies to Business Needs

Cyber security forms one of the pillars of effective information governance. Privacy regulations mandate that organizations take reasonable precautions to protect sensitive data from breach. But in an increasingly complex cyber environment, organization must move past checkbox compliance to match security measures to identified risks and cover all data platforms.

Begin with a comprehensive risk analysis to identify vulnerabilities. Then update security strategies as necessary to address weaknesses. This will include tasks such as updating password policies and incident response plans, as well as implementing appropriate encryption controls.

Additionally, an effective security strategy will address both on-premises and cloud environments. It will include endpoint protection and continuous monitoring. And it will address the human element with regular security awareness training.

Most organizations are unprepared for moving data to the cloud. A myriad of storage areas in the cloud and many default settings allow individuals to share any data with anyone in the world. Thus, some serious governance decisions need to be made. Organizations must look to safeguard sensitive data but also allow collaboration for certain groups and other types of data.

Carefully Control Access to Data

Another critical element of data security involves controlling access to data. Hackers commonly use compromised credentials to gain access to corporate data. Consequently, applying principles of least privilege and zero trust offer important protections.

For instance, tools such as Microsoft Entra help companies ensure appropriate access. By automating identity creation and updating access as employee roles change, Entra protects against privilege elevation.

Jump Start Enterprise Information Governance with Expert Guidance

Traditional information governance focuses on achieving regulatory compliance. But this reactive approach, characterized by rigid controls, can result in more obstacles than innovation. Instead, forward-thinking organizations practice adaptive information governance, using multiple governance strategies to address evolving business situations.

The consultants at Messaging Architects can help your organization identify the best next steps in building an effective information governance strategy. Whether that involves automating data classification, reviewing and updating ePolicies, addressing specific security vulnerabilities or improving data access controls, they have the tools to ease the process.