
A comprehensive strategy allows agencies to create more reliable processes for eDiscovery, increase stakeholder collaboration, and reduce risks.
Developing a comprehensive information governance strategy is the best way for agencies to better manage large amounts of data, comply with eDiscovery preservation requirements, adhere to federal records requirements, rein in costs, and respond to Freedom of Information Act (FOIA) requests in a timely manner.

Agencies have made some headway in managing all of this data in compliance with the Presidential Memorandum on Managing Government Records. But without a comprehensive, holistic information governance strategy, it’s nearly impossible to keep on top of everything, especially in the face of the growing number of unstructured data that must be managed, including email, network and cloud file storage, videos, audio files, photos, and text messages. Organizations are beginning to hear that message loud and clear: According to Gartner, 25% of organizations will manage all of their unstructured data using information governance and storage management policies by 2018, up from less than 1% today.

To understand the concept, think of a house, where each agency stakeholder has its own floor. There would be floors for IT and security, records management, legal, FOIA, and internal investigations. The data created and maintained by the agency is the common thread connecting all of its departments and stakeholders; how that data is used depends on the stakeholder. The information governance framework an agency has in place determines the house's foundation, and the strength of each stakeholder’s programs and projects relies on that foundation.

Any crack in the foundation can seriously jeopardize the structural integrity of the floors of the house and possibly cause it to crumble. While agencies have made some progress, many are still managing information in a traditional siloed approach, without input from all stakeholders. In many cases, each of these individual agency silos has its own policies, procedures, technologies, and cultural mindset.

That means that one part of the agency often has no idea how its information, policies, and procedures affect other parts of the agency. For example, a legal department, which is in charge of eDiscovery, wants to maintain maximum control over email by preserving and saving everything forever, while an IT department might develop a policy that limits users to 250 MB of email in their inboxes. The two policies aren’t in agreement, which can create chaos for both the legal team and IT because their own interests drive the rationales for their decisions. Legal is looking to limit its eDiscovery risk while IT is worried about saving money by limiting the amount of expensive storage it must purchase to keep its enterprise mail system functional.

This dynamic can come into play in other areas as well. The IT department may be in favor of the bring-your-own-device (BYOD) model to save money, but the legal team may be more hesitant from a regulatory and eDiscovery perspective because this is another policy that could be used to create discoverable information that must somehow be managed.

To successfully address and build effective solutions for these...
problems, agencies must approach information governance holistically with input from all data stakeholders. This approach, which can include consolidating various data sources into one comprehensive data store, has many benefits. Not only does it provide more reliable and efficient processes for eDiscovery, but it increases stakeholder collaboration and drastically reduces risks such as data leakage, privacy breaches, and security lapses. It also reduces costs across the board by more efficiently using agency resources and eliminating redundancy.

**Building a Strong Information Governance Foundation**

The most important criterion for a successful, holistic information governance infrastructure is strong executive-level support. This is the only way to truly close the chasm that exists between different information and cultural silos within agencies. Executive-level support also makes information governance decisions fully independent of any particular stakeholder’s needs; instead, these decisions are based on agency-wide needs and priorities.

Agencies should also build a proper business case that quantifies return on investment and justifies expenditures in terms of time, technology, and people. In addition, it’s important to look at the business case strategically, explaining how it aligns with the agency’s mission and how an information governance program will further that mission.

In addition, agencies need to make sure to involve and facilitate participation among the various data stakeholders. That means gathering input from all stakeholders about their practices for preserving litigation, records management, privacy, and data management, as well as understanding the types of technology systems they currently use.

While some of the work in building a strong, holistic information governance foundation falls under policy and procedures, much of it can be facilitated by using the right technology, from records management and information security to eDiscovery and storage/archiving tools. While researching these various technology solutions, keep in mind that there are two types: One type is a point solution that solves one specific problem and has little or no integration with other systems. More appropriate choices can function and integrate with other offerings, creating a more comprehensive governance of agency data.

**Data Archiving and Storage Optimization:** Determining where to store data is the first part of any information governance policy. There are many choices when it comes to the medium of storage, but the important part is mapping out data that may be stored in multiple repositories – email systems, document management systems, shared drives, etc. When choosing data storage and archiving tools with information governance in mind, make sure they support large amounts of unstructured data with enough flexibility and scalability to meet your long-term needs.

**Data Archiving and Storage Management:** Understanding where your data is...
Located is an important foundational brick for any information governance framework. There are many choices when it comes to the medium of storage (on premises or cloud) and the type of repository holding your valuable agency data (file shares, Sharepoint, email systems, document management systems, etc.). Leveraging data archiving and storage management tools can help agencies understand the makeup of their data, determine true custodian ownership, and know where it exists and how often it is used. This valuable information reduces an agency’s eDiscovery and cyber security exposure, saves money by reclaiming valuable disk space on high-speed production storage and archiving less-frequently accessed data to slower tier or cloud storage, and allows for a faster response to congressional inquiries and FOIA requests.

Records/Information Management: The OMB’s Managing Government Records Directive, managed by the National Archives and Records Administration (NARA), requires agencies to use automated technology for more comprehensive records management. Tools in this category automate recordkeeping, which in turn helps comply with regulatory audits. They also improve knowledge-sharing across an organization. The tools typically consist of an archiving or records management system; connectors to the most common applications and repositories; metadata enhancement and auto-classification; an analytics dashboard; a way to classify and retain records; and a method for protecting records against deletion and changes by agency employees.

Information Security/Protection: There are several important information security and protection tools that can help round out an information governance strategy by ensuring a safe network security perimeter and securing transfer of data over networks, both internally and externally, as well as safety at rest. These include malware controls, access controls, messaging and web security, endpoint protection, file-based controls, data leakage protection, encryption, authentication, data protection, and privacy controls.

eDiscovery: eDiscovery is not going away, and the problem only gets harder to solve with the proliferation of data, not only within an agency, but with data associated with cloud services and mobile devices. These advanced tools can help agencies comply with legal hold obligations, process terabytes of data, and empower users with advanced analytical and searching tools such as predictive coding and concept searching to drastically reduce investigation and document review costs and shrink the time required to wade through large volumes of data.

Benefits of the Holistic Approach
With a holistic approach to information governance, the IT department increases the manageability of the entire IT environment, thanks to a lower footprint of unstructured data and deduplication across the entire dataset. Integration with other infrastructure systems also reduces the amount of backup data being created on a
weekly basis, leading to decreased backup time and media costs. This approach allows IT to store archived or records data on less expensive disks and in cloud storage services. There are other indirect cost savings as well, including freeing up personnel to work on new projects instead of maintaining existing systems, and reducing service desk calls, since the number of end-users calling the helpdesk to restore deleted items drastically decreases.

The legal team benefits significantly with the holistic approach as well, because applying legal holds to data contained in a repository is a simple task that reduces the risk of data spoliation sanctions. This approach also helps the legal team quickly search, discover, and defensibly hold data in a repository and quickly estimate how much time and money it will take to defend or prosecute a case (early case assessment). Other benefits include:
- Reducing the amount of control a custodian has over deletion of potentially relevant data
- Eliminating pockets of unstructured or untagged data that can exist in data repositories and that hasn’t been analyzed or processed
- Performing defensible collections without requiring the assistance of IT

A more robust and comprehensive data repository allows the office of information governance/investigations team to be proactive instead of reactive when it comes to internal investigations. In addition, the OIG will spend less time investigating each case, because the data is readily accessible and because it can use eDiscovery tools for advanced analysis of the data. Across the board, a holistic approach to information governance allows agencies to respond to FOIA requests faster and more defensibly. It also allows those responsible for responding to FOIA requests to stop relying on custodial preservation and collection and to better track and document data collection tasks, in the event a question were ever to arise as to what sources were searched or how they were searched. Most importantly, a holistic approach can help agencies improve collaboration between agency counsel and FOIA professionals, thereby reducing downstream eDiscovery risk.

Finally, automating record classification – a big part of information governance – will go a long way toward meeting the 2016 and 2019 electronic records management goals detailed in the Managing Government Records Directive. In addition, the holistic approach will reduce the burden on end-users, increase the quality of preserved records, and help agencies leverage NARA’s Capstone Approach for email records management.

**Conclusion**

A holistic approach to information governance benefits agencies in many ways. Not only does it reduce risk and save money across the board, but it creates more efficient and defensible agency processes related to eDiscovery, FOIA, and records management. Most importantly, it creates a more collaborative environment where everyone can work together to put the agency’s mission first.
Symantec has an entire family of integrated solutions that give agencies the tools needed to build a strong foundation for their information governance frameworks.

**Data Insight:** A reporting, analytics, and visualization tool that helps agencies understand what data exists, how it is being used, how often it is used, who owns it, and who has access to it. Useful for determining custodian ownership for eDiscovery and FOIA purposes, as well as for insider threat and cyber security investigations.

**DLP:** A data loss prevention tool that enables agencies to monitor, protect, and manage their confidential data wherever it is stored and used, across endpoints, mobile devices, and network and storage systems.

**NetBackup:** Enterprise-class data protection for datacenters and virtualized environments. A management console reveals all backup and recovery activity, allowing consistent policies and service levels to be enforced across the agency.

**Enterprise Vault:** Market-leading enterprise archiving technology that helps agencies classify and analyze email and unstructured and structured data. Agencies can leverage this repository to reduce the storage footprint required by enterprise applications. The best way to do this is by consolidating various distinct data-source types into one system to allow for defensible preservation and searching of data for eDiscovery, FOIA, and internal investigations, and to comply with NARA Capstone Guidance to meet the 2016 goal for managing agency email records electronically.

**Mobile Device Management Suite for Agency BYOD:** Symantec Mobile Management delivers a comprehensive Mobile Device Management (MDM) solution giving public sector organizations the ability to defensibly manage and secure mobile endpoints across the entire enterprise. The solution helps protect sensitive data and applications while simultaneously reducing the risk involved with remote connectivity.

**Symantec eDiscovery Platform Powered by Clearwell:** A workflow that automates the eDiscovery process from legal hold to production, providing transparency and control. Separate modules automate the legal hold process, simplify the forensic identification and collection of electronic data from all critical data sources, and automatically cull early case assessment data by up to 90%.

---

Learn more about data security solutions at www.dlt.com/Symantec.

---

**About DLT Solutions:** Through its partnership with Symantec, DLT Solutions provides a comprehensive portfolio of solutions that address security challenges within federal, state, and local governments by helping agencies access, manage, and secure their information across the enterprise and its proliferation of end points. As a Symantec Platinum Partner, DLT holds the highest levels of authorization to assist agencies in evaluating, selecting, procuring, deploying, and supporting Symantec’s enterprise availability and information technology products such as Symantec NetBackup, Backup Appliance, Enterprise Vault, and Storage Foundation High Availability Suite. For more information, contact DLT Solutions at 800-262-4358, email edm-solutions@dlt.com, or visit www.dlt.com/Symantec.