A COBIT Approach to Regulatory Compliance and Defensible Disposal

The successful IT governance plan demands a modern and transparent approach to data retention and routine disposal. Today’s chief information officers (CIOs) face an unprecedented array of challenges:

- **Big data:** The volume of information that IT collects and manages continues to swell, constantly testing the processes and tools used to collect, analyze, store, process and archive data.
- **Globalization:** It is almost impossible today to find a large corporation operating in just one area of the world. Thousands of miles may separate an organization’s headquarters from research and development and manufacturing, while customers, partners, suppliers and satellite offices may be located around the globe. As a result, IT must support information stored in multiple locations across a diverse infrastructure of networks, servers, desktops, laptops and mobile devices.
- **Complex, evolving regulations:** More than 100,000 international laws and regulations are potentially relevant to the information collected by Forbes Global 1000 companies. This information encompasses financial records, marketing data, emails, texts, social media posts, tweets, phone records, log data and more. Even more challenging, many of these regulations, including financial disclosure requirements and standards for data retention and privacy, are continually evolving and often vary or even contradict each other across borders and jurisdictions.
- **Tight budgets:** Despite all these challenges—and the disastrous consequences of failing to successfully manage all the data and comply with regulations on a global scale—IT is under constant pressure to reduce spending.

IT can meet all of these challenges with a comprehensive, globally aware information governance program that reduces information volumes, centralizes the management of data across all jurisdictions and ensures regulatory compliance—all while reducing costs. Many CIOs already use the COBIT® framework to support business objectives, reduce corporate risk and optimize resource use. Yet, when it comes to information governance practices related to regulatory issues, legal compliance, records retention and disposal policies, COBIT principles are often not being leveraged as broadly and as effectively as possible. However, COBIT may be the key to a successful governance program.

VALUELESS CORPORATE DATA

A lack of insight into what information needs to be kept has led many organizations to accumulate mountains of electronically generated debris in the form of excess applications, servers, storage and backup tapes that no longer have any utility.

A recent survey of corporate CIOs and general counsels conducted at a Compliance, Governance and Oversight Council (CGOC) summit found that typically only 1 percent of corporate information is on litigation hold, only 5 percent is in a records retention category and a mere 25 percent has any current business value. This means that approximately 69 percent of all the data collected and maintained by most organizations have no business, legal or regulatory value at all.

A key step in creating a successful information governance program is developing the ability to identify and protect any information that has business, legal or regulatory value in order to support the legally defensible disposal of everything else. Effective defensible disposal—the ability to regularly and automatically eliminate information that has no regulatory, legal or business value—can have a dramatic effect on reducing costs and improving compliance.
impact on information economics. Less IT budget spent on storage, servers and backup means that more can go to strategic investments. Less information to sift through means that the legal and regulatory response can be handled in a streamlined and efficient fashion while minimizing the risk associated with keeping too much or too little data, including retaining information that evolving privacy regulations require be eliminated and unnecessarily providing opposing counsel with broader discovery access than required. Less wasteful information management ultimately allows corporations to return more profit to shareholders.

Historically, retention schedules have included only records—whether paper or electronic—that are distinct from the rest of the information in the organization. To achieve defensible disposal, IT stakeholders must be able to collaborate closely and transparently with the records and information management (RIM), legal and business units to create modern executable retention schedules—schedules that go beyond the scope of setting retention periods. What is deemed a “record” should include all information in the organization and incorporate retention criteria related to legal holds and business value.

**RETENTION SCHEDULES IN A DIGITIZED WORLD**

A retention schedule provides the legal foundation for records management and legal departments to organize corporate records and information and then detail the length of time that such records must be retained for compliance and business needs. The problem is that the retention schedules used by many organizations today were devised when paper records were the norm. Thus, they simply do not work in today’s enterprises because a large amount of the information that needs to be retained or deleted is electronically generated and includes information historically defined as a record, e.g., social media posts and tweets. This creates a critical disconnect because the information is now under the domain of IT and the company’s compliance obligations will need to be linked to the thousands of applications, databases and other repositories IT manages.

Meanwhile, legal and RIM professionals possess the knowledge to set retention schedules and disposal policies according to relevant laws and regulations, but they may not have a holistic view of the IT infrastructure or any understanding of the business value of existing information. Relevant data should be identified and there should be a mechanism for disposing of information.

This disconnect is highlighted in the CGOC survey, which reported that:

- Seventy-seven percent of respondents said their retention schedules were not actionable for business and IT staff
- Fifty percent said their IT departments did not use the retention schedule
- Seventy-five percent cited an inability to defensibly dispose of data as one of their greatest challenges, and many highlighted massive volumes of legacy data as financial drags on the business and compliance hazards

The goal of creating a modern, transparent and executable retention schedule is to overcome these challenges by facilitating the identification of valueless information and automating its disposal in a legally defensible manner.

**BUILDING A BETTER RETENTION SCHEDULE WITH COBIT**

Because a modern, executable retention schedule recognizes the dynamic nature of electronic data and the shared responsibility for information management and disposal, COBIT principles provide a solid foundation for creating one.

COBIT® 5 is based on five key principles for the governance and management of enterprise IT:

1. Meet stakeholder needs.
2. Cover the enterprise end-to-end.
3. Apply a single, integrated framework.
4. Enable a holistic approach.
5. Separate governance from management.

All of these principles are directly applicable to the creation of a modern and executable retention schedule that supports a legal framework for defensible disposal of unneeded data and takes into account the needs and roles of legal, RIM, business and IT stakeholders by:

- Understanding the flow of information through the enterprise—from creation to disposal—and enabling a holistic approach to information management
Recognizing the multidimensional nature of data retention and disposal, and supporting interdependencies and collaboration among key stakeholders to meet all legal, regulatory and business requirements

Having integrated governance policies and processes in place to meet the varied and diverse stakeholder needs, achieve global compliance, and enable regular updates to stay abreast of changes in the law and the business

Making day-to-day management of information more efficient and compliant with transparent and clearly defined governance policies and processes

In such an environment, users would have the knowledge and tools they need to classify information, and IT would have the legal and records support it needs to implement a workable retention schedule and appropriately dispose of valueless information at the right time.

The following are the key elements that must be incorporated into a retention schedule for it to work in the modern information age:

1. **Apply retention schedules to all information, not just records.** The retention schedule must reflect the ongoing convergence of records management and data management and apply to all data in an organization’s possession. Classify all information—including structured and unstructured data sources—as either having legal, regulatory or business value or as debris.

2. **Connect specific legal, privacy and regulatory retention obligations directly to relevant information.** The retention schedule must be supported by a transparent global framework that clearly defines how legal and regulatory obligations apply to all types of information and business users, including structured and unstructured data sources—as either having legal, regulatory or business value or as debris.

3. **Take into account the business value of information.** This value must be explicitly determined by business stakeholders and made transparent to legal, RIM and IT. Again, technology solutions now exist that can address this long-standing concern of enterprise data managers by helping users to more easily associate information types (e.g., purchase orders or employee agreements) with specific data sources (e.g., ECM and HR systems or applications like Microsoft SharePoint) and include details on why the information is of business value and for how long.

4. **Identify where information is located.** The retention schedule should include information inventories describing where information is stored, what record classes apply to specific repositories, who was and is responsible for the content, and who manages it. With the help of a reliable data map, data stewards can more easily identify information and understand the value and obligations related to that information according to, for example, lines of business or departments.

5. **Communicate retention and disposal obligations in a language that stakeholders can understand.** This involves two elements. First, data users must know what is required of them when creating and identifying information. Second, data stewards must understand their responsibilities related to the disposition of information. For example, IT staff might not make sense of a disposition directive that states, “Comply with record class HUM100.” A useful translation might be: “Job applications created by human resources (HR) users and stored on the shared HR drive must be permanently deleted 10 years after the termination of the employee.” Clarity encourages compliance.

6. **Build in the flexibility to adapt to local laws, obligations and limitations.** Business users in each functional area and jurisdiction are the most knowledgeable about the value in, and purpose of, the information they create. The retention schedule must have the flexibility to incorporate this local knowledge. In addition, retention schedule technology solutions can be used to catalog all the specific laws and regulations in applicable regions and jurisdictions so that various exceptions and changes can be incorporated into the retention schedule and communicated to the relevant stakeholders to ensure compliance on a global scale.
7. Include an actionable mechanism that allows legal and IT to collaborate in executing and terminating legal holds. No retention schedule can achieve the goal of defensible disposal without a clear understanding of what information is subject to legal hold and when the hold has been released. Understanding the physical location of the information is essential, particularly for rigorous protocols such as mandated videotaped shredding of hard disk drives. With linkages clearly established between information value and IT systems, legal departments can syndicate legal holds from around the world and identify relevant records and information with local schedules and individual records flagged and held.

8. Identify and eliminate duplicate information. Confusion about what exactly needs to be retained and for how long can invite a tendency to “save everything, just in case.” In addition to conflicting with the increasing number of privacy laws (e.g., the US Health Insurance Portability and Accountability Act, the European Directive on Protection of Personal Data) that require the deletion of certain types of information, saving everything means that tens or even hundreds of copies of the same file are being retained. Through a transparent governance and management framework, companies can be confident they have retained the required information and disposed of all unnecessary copies.

9. Update in real time to account for changes in laws to the business and in technology. With the constant evolution of global legal, regulatory and privacy requirements, it is vital to stay ahead of changes and incorporate new requirements into the retention schedule immediately. Technology solutions can automatically update systems and alert data stewards to relevant changes. Several major legal research database providers also offer tools that enable users to track changing laws.

10. Automatically apply retention schedules and legal holds to data sources that are now capable of receiving instructions from automated policy tools, and instrument all retention and disposal processes. This ensures the consistent disposition of unnecessary data, enables legal and RIM to validate hold requests and compliance efforts, and allows information governance leaders to monitor and improve the defensible disposal program.

GOOD GOVERNANCE ACROSS THE INFORMATION LIFE CYCLE

Unprecedented data growth, global business operations, cost concerns, and a complex and constantly changing regulatory environment have created daunting information governance challenges for CIOs. However, the COBIT framework makes it possible to apply proven governance principles to overcoming these challenges by efficiently and cost-effectively shepherding the flow of corporate information through its useful life cycle and automatically eliminating information that no longer has any legal, regulatory or business value. By collaborating with legal, RIM and business stakeholders, IT can also help to create a modern, transparent and executable retention schedule that can ensure compliance while increasing business agility, reducing risk and lowering costs through the defensible disposal of valueless information.

ENDNOTES

1 The Compliance, Governance and Oversight Council (CGOC), founded by Deidre Pakrad, director of information life cycle governance at IBM Corporation, is a forum of more than 1,900 legal, IT, records and information management professionals from corporations and government agencies.


3 Ibid.