Information Governance

San Jose State University

Susan Wolfe
MARA 284
October 6, 2013
Abstract

Sarbanes-Oxley Act (SOX 2002) is considered to be one of the triggers for the rise of information governance. The need to comply with SOX has had a cascading effect on corporate governance strategies. Information governance incorporates multiple disciplines (e.g., records and information management, risk management, knowledge management, and e-discovery protocols). Without collaboration and unified governance an organization leaves itself open for skyrocketing costs, and increased risk, as well as possibly losing potential return on investment. Information governance is a holistic approach to identifying the hidden value of information assets that may be overlooked if viewed only through the lens of records retention schedules.

Keywords: Information Governance, Records and Information Management, Information Assets
Information governance incorporates multiple disciplines (e.g., records and information management, risk management, knowledge management, and e-discovery) to effective and efficient use of information by organizations (Baron, 2011). The Sarbanes-Oxley Act (SOX 2002) is considered to be one of the triggers for the rise of information governance. The need to comply with SOX has had a cascading effect on corporate governance strategies (Heroux & Fortin, 2011).

An information governance [IG] framework has four parts: people, policies, technology, and risk management. Attention must be paid to all parts equally, as it is easy to develop a framework that incorporates only policies, technology, and risk, excluding the human element in the program. The goal of IG “is two-fold: compliance and value creation” (Samuelson, 2010, p. 2). There is a need for comprehensive IG strategies that include people and organizational knowledge. It is in this way assets can be reused, productivity increased, and organizations will not find themselves reinventing the wheel every time they begin a new endeavor.

Information governance programs can support business processes by improving information-related workflow practices and through the reduction of possible security, privacy, and compliance risks. Information should not be seen only as a potential liability that should be destroyed at the earliest opportunity. Information is also beneficial to organizations. Information governance is a holistic approach to identifying the hidden value of information assets that may be overlooked if viewed only through the lens of records retention schedules. Effective IG can protect an organization from risk as well as provide a greater return on investment for records and information management programs (Baron, 2011).
Analysis

Over the course of the last decade, we have firmly transitioned into what Forrester Research Group terms the new ‘data economy’ (Goetz, 2013). Because of increasing competition from a global economy, new information-centered business models, and a shifting regulatory environment, the need for a comprehensive, outcome-oriented, and business-driven information governance practices has arisen (Goetz, 2013).

Organizations can experience negative consequences as a result of not having an IG program in place. When there is more information to store, there can be an increased cost in IT expenditures in order to deal with the increase in data. With large amounts of unstructured data, this also can mean increased costs associated with eDiscovery requests (Murphy, 2013).

In the data economy, organizations that have no formal IG program are possibly managing projects that are aligned with unit operational-goals instead of business-goals. For example, a global machinery manufacturer required managers to provide C-level executives with a projected ROI across strategic and operational performance areas. The data projects necessary to obtain these estimated returns were being treated as project-based, and the manufacturer was affected by cost overruns as a result of the increased information management. When an IG program was implemented, the manufacturer could see the interdependence of information needs and the information governance oversight. The financial services business unit could then predict the cost-per-project and could provide adequate funding for data reviews without falling short of its projected profits (Goetz, 2013).

Without an IG program in place, organizations may have the inability to leverage
corporate knowledge assets. Organizations have interest in information assets in proportion to their relative value to help drive the profit or the purpose of the organization itself. Once an asset stops returning profit or support for the purpose, then the organization “quickly loses interest in managing it, cleaning it up, or paying for it to be stored” (“Using the IGRM Model,” 2012, para. 5). The increased costs associated with the loss of these organizational assets are not only purely capital losses; an organization also loses the productivity of its human capital as they try to locate an asset lost in a asset management systems. As the asset needs to be recreated again instead of being reused or reallocated, the production costs continue to rise (Murphy, 2013).

Reused and repurposed assets increase efficiency and reduce redundancy because no one person has the expertise necessary to conduct a strategic information value assessment alone, experts from across the organization, including data governance, business intelligence, enterprise content management, knowledge management, and records and information management (Baron, 2011). It is not sufficient to focus solely on the return on investment in IG policies within knowledge-based organizations. Intellectual capital is an intangible resource. In order to establish an information governance program, organizations must be able to: identify the core activities of knowledge-workers, measure the financial impact of their activity, and identify the service or practices of knowledge-workers (Breunig & Hydle, 2011).

IG programs can protect an organization from increased exposure to risk by allowing it to respond agilely to shifting market trends, leveraging organizational assets to maintain a competitive advantage (Murphy, 2013). Several years ago, a Canadian utility provider, discovered that a lack of control over information assets, especially
email, was putting the company at risk. As a solution to the problem, the records management function was moved from legal to IT. A new position, manager of strategic information management, was created. The IT department then split into two business units: IT Operations and IT Governance. This new information governance program, designed by Sam McCollum, was "an accountability framework that includes the people, processes, policy and technology that ensure the effective management of information to enable an organization to achieve its strategic goals and business programs" (Raths, 2013, para. 4).

Organizations without an IG program in place face compliance processes that move beyond a single business unit. The complexity of unstructured data and information stored in multiple systems means that organizations face an inability to efficiently manage legal holds, and/or to identify personally identifiable information (Murphy, 2013). Unstructured data generally resides in a file storage system and the metadata about the file resides in a relational database. Examples of unstructured data include documents, email, IMs, and social media content. Unstructured data comprises of 80-85% of an organization’s information assets, and McKinsey Global Institute projects this percentage to grow by 40% in volume per year (Murphy, 2013).

Organizations are usually better at managing structured data than unstructured data. If an IG program is not implemented, information assets stored as unstructured data can be underutilized, or worse, personally identifiable information stored as structured data could be at risk. Information governance programs seek to realize the benefits of their information assets while at the same time reduce potential risk (Baron, 2011).
Conclusion

Over the last few decades, the need for organizations to actively manage their records and information assets has grown exponentially. It is no longer a matter of choice, for the sake of a competitive edge, or to solely minimize risk. The need for information governance has arisen out of a need for cross-functionality across business units; international trade, local, state, national, and international regulations; and the recognition that knowledge resides in the experience of the individuals that make up the organization. In order to successfully design IG programs within organizations, one must take a broad approach that includes financial control, strategic planning, resource management, and both structured and unstructured knowledge that resides within the organization (information governance, 2011).

Records and information managers together with legal are tasked with managing risk for organizations. This can be done with an effective records management program that clearly identifies records series, retention, and disposition requirements (including long-term archival value). Information technology managers are responsible for maintaining the IT systems that store and maintains an organization’s information assets. IT duties include managing privacy and security requirements that are dictated by records and legal. It is the goal of IT to increase the efficiency of the system, which in turn will lower the costs to the organization. Records managers and legal can identify the value and purpose of information assets to an organization; IT uses their guidance to manage and maintain a system that meets the policies set in place. Without collaboration and unified governance an organization leaves itself open for skyrocketing costs, and increased risk, as well as possibly losing potential return on investments.
References


