The Sedona Conference Journal

Volume 15 2014

The Sedona Conference Commentary on Information Governance

The Sedona Conference

Recommended Citation:

The Sedona Conference, *Commentary on Information Governance*, 15 SEDONA CONF. J. 125 (2014), https://thesedonaconference.org/publication/Commentary_on_Information_Governance.

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual basis, containing selections from the preceding year's Conferences and Working Group efforts.
The Journal is available on a complementary basis to courthouses and public law libraries and by subscription to others ($45; $30 for Conference participants and Working Group members).
Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our Conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference, 5150 North 16th Street, Suite A-215,
Phoenix, AZ 85016 or call 1-602-258-4910; fax 602-258-2499; email info@sedonaconference.org.

The Sedona Conference Journal® designed by MargoBDesign.com – mbraman@sedona.net

Cite items in this volume to "15 Sedona Conf. J. _____ (2014)."

THE SEDONA CONFERENCE COMMENTARY ON INFORMATION GOVERNANCE*

A Project of The Sedona Conference Working Group on Electronic Document Retention & Production (WG1)

Author:
The Sedona Conference

Editor-in-Chief
Conor R. Crowley

Drafting Team

Keith M. Angle
Jason R. Baron
Christopher Beahn
Bennett B. Borden
Howard Feldman
Liam A. Ferguson
Dean Gonsowski
Jack Halprin
Tim Hart
Virginia H. Johnson
Wayne C. Matus
Tim Noonan
Cheryl Pederson
Charles R. Ragan
Jim Shook
Peter Sloan
David L. Stanton
Cheryl Strom
Jeane A. Thomas

Thanks go to all who participated in the dialogue that led to this Commentary. We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors just click on the "Sponsors" Navigation bar on the homepage of our website.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

PREFACE

Welcome to The Sedona Conference *Commentary on Information Governance*, a project of The Sedona Conference Working Group One on Electronic Document Retention & Production (WG1). WG1 is best known for its ground-breaking publication, *The Sedona Principles* Addressing Electronic Document Production, and as such, is generally associated in the minds of legal professionals and the public at large with civil litigation, and more specifically, with electronic discovery. But when *The Sedona Principles* were being drafted ten years ago, members of WG1 immediately recognized that no discussion of electronic discovery in civil litigation was complete, or even possible, without a discussion of the records and information management context from which requests for and responses to electronic discovery emanate. As a consequence, *The Sedona Principles* have been augmented over the past decade by WG1 commentaries that discuss the management of electronic information in the day-to-day conduct of business, government, and private life. These commentaries have included:

- *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*
- *The Sedona Conference Commentary on Email Management*
- *The Sedona Conference Commentary on Inactive Information Sources*
- *The Sedona Conference Primer on Social Media*
- *The Sedona Conference Best Practices Commentary on Search & Retrieval Methods*
- *The Sedona Conference Commentary on Finding the Hidden ROI in Information Assets*

With the exception of the final title in the above list, one could still sense in all these commentaries that the litigation risk management tail might be wagging the information management dog. The final Commentary on *Finding the Hidden ROI in Information Assets* broke cleanly with that history, initiating a discussion that went beyond managing the e-discovery risks associated with information, to better leverage the enormous value of information that is caught up within firms and organizations of all types.

We now take the next step, and that is to define Information Governance as an organization's coordinated, interdisciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value. In drafting this Commentary, it has been the mission of WG1 to bring together lawyers, records and information managers, technical experts, privacy and security professionals, business process engineers, human resource officers, and others, to develop a comprehensive set of basic principles to guide the development and operation of a robust Information Governance program in any organization.

The Commentary represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I wish to thank everyone involved in devoting their time and attention during the drafting and editing process, and in particular Keith Angle, Jason Baron, Dean Gonsowski, Tim Hart, Wayne Matus, Cheryl Pederson, Chuck Ragan, Jim Shook, Peter Sloan, David Stanton, and Cheryl Strom. I especially acknowledge the tireless evangelism of Editor-in-Chief Conor R. Crowley, who not only spent countless hours on the draft of this Commentary but also patiently explaining the concept of Information Governance to sometimes resistant stakeholders, helping them break out of their professional "silos" and recognize the need for a broader vision.

The Commentary represents the collective wisdom of a score of highly-qualified Information Governance professionals who contributed to the draft. The members of The Sedona Conference Working Group Series were able to review and comment on this Commentary prior to publication, it was presented at the 2013 Georgetown Law Center eDiscovery Institute, and it benefited from a six-month public comment period. But Information Governance is still very much an evolving concept. The drafters and contributors all agree that through shared experience and dialogue, Information Governance will mature as a discipline, necessitating a second edition of this Commentary. You are invited to join the dialogue online at https://thesedonaconference.org or submit comments by email to info@sedonaconference.org.

Kenneth J. Withers
Deputy Executive Director
The Sedona Conference
October 2014

TABLE OF CONTENTS

THE SEDONA CONFERENCE PRINCIPLES OF INFORMATION GOVERNANCE

1. Organizations should consider implementing an Information Governance program to make coordinated decisions about information for the benefit of the overall organization that address information-related requirements and manage risks while optimizing value.

2. An Information Governance program should maintain sufficient independence from any particular department or division to ensure that decisions are made for the benefit of the overall organization.

3. All information stakeholders should participate in an organization's Information Governance program.

4. The strategic objectives of an organization's Information Governance program should be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities.

5. An Information Governance program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.

6. The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.

7. When information governance decisions require an organization to reconcile conflicting laws or obligations, the organization should act in good faith and give due respect to considerations such as privacy, data protection, security, records and information management, risk management, and sound business practices.

8. If an organization has acted in good faith in its attempt to reconcile conflicting laws and obligations, a court or other authority reviewing the organization's actions should do so under a standard of reasonableness according to the circumstances at the time such actions were taken.

9. An organization should consider reasonable measures to maintain the integrity and availability of long-term information assets throughout their intended useful life.

10. An organization should consider leveraging the power of new technologies in its Information Governance program.

11. An organization should periodically review and update its Information Governance program to ensure that it continues to meet the organization's needs as they evolve.

EXECUTIVE SUMMARY

Information is crucial to modern businesses. Information can have great value, but also pose great risk, and its governance should not be an incidental consideration. Despite these realities, there is no generally accepted framework, template, or methodology to help organizations make decisions about information for the benefit of the organization rather than any individual department or function.

"Information Governance" as used in this Commentary means an organization's coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value. As such, Information Governance encompasses and reconciles the various legal and compliance requirements and risks addressed by different information-focused disciplines, such as records and information management ("RIM"),[1] data privacy,[2] information security,[3] and e-discovery.[4] Understanding the objectives of these disciplines allows functional overlap to be leveraged (if synergistic); coordinated (if operating in parallel); or reconciled (if in conflict).[5]

The position of The Sedona Conference is that Information Governance should involve a top-down, overarching framework, informed by the information requirements of all information stakeholders that enable an organization to make decisions about information for the good of the overall organization and consistent with senior management's strategic directions.

This paper explains the need for a comprehensive approach to Information Governance. The paper addresses:

- Why traditional, siloed approaches to managing information have prevented adequate consideration of information value, risk, and compliance for the organization as a whole;

---

1 **Records and Information Management** is the standardized process to create, distribute, use, maintain and dispose of records and information, regardless of media, format or storage location, in a manner consistent with an organization's business priorities and applicable legal and regulatory requirements. RIM principles also provide for the temporary suspension of policies or processes that might result in the deletion of records or information subject to a legal hold.

2 **Data Privacy** is the right to control the collection, sharing and destruction of information that can be traced to an individual. In general, data privacy is more comprehensively protected outside of the United States, particularly in the European Union member states, where the Data Protection Directive provides significant restrictions on the processing and transfer of personal data, and other countries including Argentina, Canada, Israel, Switzerland and Uruguay. *See* Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31. In the US, the approach to data privacy is generally contractual, and does not enjoy the same level of generic legal protections. Disparate laws in the United States do, however, mandate protections for specific types of data or target different groups. Examples include: patient records under the Health Insurance Portability and Accountability Act ("HIPAA"), financial information under the Graham-Leach-Bliley Act ("GLBA"), and prohibitions on the collection of information about children younger than 13 years old, under the Children's Online Privacy Protection Act ("COPPA").

3 **Information Security** is the process of protecting the confidentiality, integrity, and availability of information and assets, enabling only an approved level of access by authorized persons, and properly disposing of such information and assets when required or when eligible. Information security often focuses on limiting access to certain types of information that is important to the organization by restricting access through various controls including physical safeguards, technical access controls (e.g., permissions to Read, Write, Modify, Delete, Browse, Add, and Rename), authorization challenges (e.g., usernames and passwords) and encryption technologies. Security requirements can be mandated by law (e.g., HIPAA Security Rule), by contract, by industry requirements (e.g., PCI) or simply by company requirements and best practices.

4 **Electronic Discovery** ("e-discovery") is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing electronically stored information ("ESI") relevant to pending or anticipated litigation, or requested in government inquiries. E-discovery includes gathering ESI from numerous sources, reviewing and analyzing its relevance and the applicability of any privileges or protections from disclosure, and then producing it to an outside party.

- How hard costs, soft costs, opportunity costs, and risk accumulate for organizations lacking adequate control of information;

- The definition of Information Governance, its fundamental elements, and the resulting benefits to the organization; and

- The crucial role of executive sponsorship and ongoing commitment.

THE INFORMATION GOVERNANCE IMPERATIVE

We live and work in an information age that is continually – and inexorably – transforming how we communicate and conduct business. Regardless of an individual organization's size, mission, marketplace or industry, information is a crucial asset for all organizations; and if inadequately controlled, a dangerous source of risk and liability.

Some examples illustrate the highly public repercussions of information control lapses:

- Significant and increasing costs of complying with e-discovery obligations;

- Data privacy and security breaches, such as a global electronics company attributing $171 million in out-of-pocket remediation costs to a data breach affecting 100 million persons, with the total harm, including reputational injury, estimated to exceed $1 billion;[6]

- E-discovery sanctions, such as an award of $8.5 million in monetary sanctions against patent holder for willfully failing to produce tens of thousands of discoverable documents;[7]

- Recordkeeping compliance penalties, such as a national clothing retailer fined over $1 million by the U.S. Immigration and Customs Enforcement Agency for information compliance deficiencies in its I-9 employment verification system, and a retail pharmacy chain reaching an $11 million settlement with the U.S. Government for record-keeping violations under the Controlled Substances Act.[8]

Behind the headlines, however, is a more pervasive problem – the commonly unmeasured aggregation of hard costs, soft costs, opportunity costs, and risk borne by organizations that fail to effectively control their information.

---

5 *See* Appendix A for additional discussion of the intersections of these disciplines.

6 Mathew J. Schwartz, *Sony Data Breach Cleanup to Cost $171 Million*, INFORMATIONWEEK SECURITY, May 23, 2011, http://www.informationweek.com/security/attacks/sony-data-breach-cleanup-to-cost-171-mil/229625379.

7 *Qualcomm, Inc. v. Broadcom Corp.,* No. 05cv1958-B (BLM), 2008 WL 66932 (N.D. Cal. January 7, 2008) *vacated in part by Qualcomm v. Broadcom Corp.,* No. 05CV1958-RMB (BLM), 2008 WL 638108 (N.D. Cal. March 5, 2008); *see also Day v. LSI Corp.*, No. CIV 11–186–TUC–CKJ, 2012 WL 6674434 (D. Ariz. Dec. 20, 2012) (awarding partial default judgment and attorney's fee award of $10,000, resulting from the loss of information that should have been retained according to both a document retention policy and a litigation hold that was not properly enforced); *Pillay v. Millard Refrigerated Servs., Inc.*, No. 09 C 5725, 2013 WL 2251727 (N.D. Ill. May 22, 2013) (issuing adverse inference instruction against a company for failing to stop the automatic deletion of employee productivity tracking data, which it had used as a reason for terminating a disabled employee).

8 Immigration and Customs Enforcement, Department of Homeland Security, *Abercrombie and Fitch Fined after I-9 Audit*, (2010), http://www.ice.gov/news/releases/1009/100928detroit.htm (last visited Nov. 13, 2013); Debbie Cai, *DOJ: CVS to Pay $11 Million to Settle Claims of Bad Record-Keeping*, THE WALL STREET JOURNAL, (April 3, 2013), *available at* http://online.wsj.com/article/BT-CO-20130403-710237.html.

Knowingly or not, organizations face a fundamental choice: they can control their information, or by default, they can allow their information to control them.

Siloed Approaches Fail to Govern Information

Many organizations have traditionally used siloed approaches when managing information, resulting in decisions being made without sufficient consideration of information value, risk, or compliance for the organization as a whole. Examples of these silos include the various departments or administrative functions within the organization that deal with the organization's information, such as IT, Legal, Compliance, Records and Information Management, HR, Finance, and the organization's various business units. Each business unit or administrative function commonly has its own information governance policies and procedures, as well as disparate data systems and applications.

Another type of information silo consists of those disciplines that deal with specialized categories of information issues, such as data privacy and security (focused on protection of regulated classes of information), litigation e-discovery (focused on preservation and production of information in litigation), and data governance[9] (focused on information reliability and efficiency). Over time, these disciplines have developed their own terminologies and frameworks for identifying issues and addressing specific information challenges.

The core shortcoming of the siloed approach to governing information is that those within particular silos are constrained by the culture, knowledge, and short-term goals of their business unit, administrative function, or discipline. They perceive information-related issues from the vantage point of what is familiar and important specifically to them. They often have no knowledge of gaps and overlaps in technology or information in relation to other silos within the organization. There is no overall governance or coordination for managing information as an asset, and there is no roadmap for the current and future use of information technology.

Siloed decisions concerning information often have unintended consequences for the organization as a whole, with significant cost and risk repercussions:

- An organization's individual business units independently make decisions about implementing information technology tools and systems, separate from the other business units. This results in duplication of technology and unneeded expense, and also prevents the efficient sharing of information, a valuable asset, across the organization.

- The IT Department establishes email account volume limits to relieve operational stress on an organization's email system. This results in personnel

9 We recognize that various definitions of "information governance" have been advanced (*see e.g.,* Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 RICH. J.L. & TECH. 12 at 30-33 (2013), *available at* http://jolt.richmond.edu/v19i4/article12.pdf, and that there is an emerging discipline called "data governance," and submit that data governance is a subset of our information governance concept. The Data Governance Institute, self-described as a mission-based and vendor neutral authority on essential practices for data strategy and governance, defines "data governance" as "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods." *Definitions of Data Governance,* THE DATA GOVERNANCE INSTITUTE, http://www.datagovernance.com/adg_data_governance_definition.html (last visited Nov. 13, 2013). So viewed, "data governance" does not address "why" an organization chooses to do certain things with its data and other information; that is the critical role of Information Governance, ensuring that actions users take with information-related assets is consistent with organizational strategy.

moving email to storage on local drives and devices, exacerbating both data security risks and difficulties in finding and preserving such email for litigation.

- Legal counsel issues overbroad litigation holds to avoid even a remote possibility of spoliation sanctions. This results in excessive costs in pending and future litigation and also the unnecessary retention of data.

- Personnel are allowed to conduct an organization's business on their own laptops and smartphones, under a Bring-Your-Own-Device ("BYOD") program to increase convenience and efficiency but without sufficient BYOD policies and controls or planning for natural attendant consequences. This results in data security exposures and difficulties in applying records retention policies and in preserving and collecting data for litigation.

- Privacy and data security controls are applied to an organization's service providers, but are not used to ensure that service providers also meet the organization's records retention requirements. This may result in inconsistent application of such requirements to records.

- Records manager initiates a robust data and email retention program without regard to potential technological limitations or the burden associated with retaining, searching and reviewing the resulting data for e-discovery purposes.

In the post-Sarbanes-Oxley world, many companies have adopted codes of conduct, in which they broadly proclaim that the organization and its employees comply with all applicable laws (including privacy and data security requirements), protect confidential information, use electronic communications wisely, and follow procedures for retaining records. The siloed approach to addressing information issues, however, inevitably spawns a multitude of information-related policies adopted though various projects and initiatives. Thus, rather than a clear, uniform set of information policy guidance, employees face a cacophony of conflicting policies and procedures, making compliance virtually impossible in the heat of a competitive business environment, and negatively impacting productivity.

The "elephant in the room" is the organization's need to harness and control its information, coupled with the inadequacy of a siloed approach for accomplishing this crucial goal. The solution to this quandary is for organizations to find a way to bridge across their silos, so that issues of information compliance, risk, and value can be identified, understood, and addressed for the benefit of the entire organization.

Information Governance

"Information Governance" as used in this Commentary means an organization's coordinated, inter-disciplinary approach to satisfying information legal and compliance requirements and managing information risks while optimizing information value. Organizations that adopt Information Governance programs are able to bridge across silos, thereby perceiving and understanding information-related issues from the perspective of the overall organization. Information Governance also helps ensure that decisions and solutions regarding information compliance, risk controls, and value optimization will serve the needs of the entire organization rather than the insular needs of individual silos.

To accomplish Information Governance, organizations should:

- Establish a structure for Information Governance, which will vary in form depending on the organization's size, complexity, culture, and industry and regulatory environment;

- Determine the organization's strategic objectives for Information Governance, based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities;

- Reconcile the various compliance requirements and risks addressed by different information-focused disciplines, such as records and information management, privacy, data security, and e-discovery; and

- Implement an Information Governance program with the structure, direction, resources, and accountability to provide reasonable assurance that the program's strategic objectives will be achieved.

The Benefits of Information Governance are Significant

The advantages of establishing an Information Governance program are many and varied, depending upon the information-related issues and risks an organization faces. Beyond addressing the risks above, an enterprise-wide Information Governance program will help organizations achieve the following advantages, all of which add to the bottom line:

- Business performance improvements, as users gain confidence that they can locate valuable information efficiently and reliably, and better understand how to address information-related risks;

- Realization of "option value" as the organization leverages existing information and technologies across diverse business units, consolidates technologies and administrative staff, and reduces license fees;

- More reliable and efficient processes and procedures for e-discovery;

- Reduced storage costs and administrative burdens, as obsolete and worthless information is eliminated; and

- Reduced costs and enhanced compliance with legal obligations for records retention, privacy and data security, and e-discovery, as information policies and processes are rationalized, integrated, and aligned in accord with the organization's information governance strategy.

Senior Leadership Support is Essential

The commitment of senior leadership is crucial for organizations to be successful in adopting Information Governance. Such ongoing commitment is particularly important given the challenge of effectively bridging across existing organizational silos.

Thus, senior leadership should sponsor and firmly support the organization's Information Governance efforts by:

- Endorsing the importance of Information Governance to the entire organization;
- Chartering a structure of responsibility and accountability for implementing an Information Governance program;
- Adopting or approving the strategic objectives of the Information Governance program;
- Providing appropriate resources to implement and sustain the Information Governance program;
- Establishing a supportive "tone at the top" and an environment in which Information Governance remains an organizational priority; and
- Ensuring that the Information Governance program is administered consistent with its objectives and is periodically reviewed and updated.

There is often a balance of value against cost or risk that changes over time for a given information asset. Organizations may leverage information effectively over the short term, but once the data's short-term use is expended, the data is often stored away and rarely reassessed for any long-term strategic value. Left ungoverned, this potentially valuable asset is not only wasted, it also may become a significant liability. Through proper information governance, organizations can realize additional benefit from their information assets over time while reducing risk.

The Business Case for Information Governance

Multiple business cases can be established for pursuing Information Governance. Successful adoption of the information governance approach requires both strategic commitment (adoption of information governance as an organizational priority) and also tactical efforts (such as specific projects to establish and implement the program). A business case will be needed, both to support the strategic commitment and also to justify the expenditures of time, effort, and funding required for specific implementation projects. Because the business case for information governance must be persuasive at both strategic and tactical levels, the business case should include both strategic (qualitative) and project-based (quantitative, ROI) elements.

The Strategic/Qualitative Business Case:

Information governance is an ongoing program that evolves over time through maturity levels. As such, it is unrealistic to attempt to comprehensively quantify all of its benefits. One might just as easily attempt to exhaustively measure all benefits of managing the organization's tangible or people assets. ROI analysis is best used for applications of information governance to specific, issues or projects within the information governance initiative, as discussed in Appendix D.

At a strategic level, the business case should instead convey how information governance aligns with and amplifies the core values and fundamental, strategic objectives of the organization. For example:

- **Low Cost Provider**

Companies singularly focused on operational efficiency and cost control, such as in low-margin, high-volume industries or market segments, may adopt information governance to streamline information workflows and reduce unnecessary information storage and retention, thereby reducing costs and increasing business efficiency.

- **Innovative Excellence**

Organizations driven by creative innovation and excellence in products and services may adopt information governance to maximize the value of their information assets, helping them capture valuable information for innovative repurpose while minimizing the distraction of unnecessary information.

- **Trusted Provider/Advisor**

Organizations with the core value and brand of being a trusted business provider or advisor may adopt information governance to strengthen their protection of information that customers or clients entrust to the organization and also to enhance third-party perceptions of the organization as a trusted custodian for such information.

- **Integrity/Ethics**

Companies, including publicly traded organizations and those in highly-regulated industries, may adopt information governance as a complement to their internal control systems and corporate ethics and integrity programs to ensure information-related legal compliance and risk management.

In each of the above examples, information governance provides specific, tangible benefits that often can be quantified on an ROI basis as discussed below. Yet, in each example, information governance also amplifies the organization's core value of choice, by ensuring that information is handled in alignment with the strategic value or brand. This alignment allows information governance to reinforce the particular organization's fundamental values, as information is managed in a way that "walks the walk."

Conversely, information governance also helps organizations avoid cultural dissonance for their core values, such as, for example, the "low cost provider" that squanders money on information inefficiency and unnecessary retention; the "innovative excellence" company that fails to optimize the value of its information; the "trusted partner/provider" that is careless with the information entrusted to it; or the company espousing "integrity and ethics" that fails to establish a control environment for information as a valuable asset and as a means to detect and prevent compliance lapses. Thus, adoption of information governance can have profound, strategic significance beyond the quantitative ROI measures mentioned below and considered in more detail in Appendix D.

The Quantitative/ROI Business Case:

A typical ROI analysis weighs the benefits of a particular project against its cost, and calculates the length of time it will take to recoup the cost. The quantitative aspects of the business case are best determined by focusing on specific applications of information governance to identified problems or opportunities, or to discrete projects for implementation of the Information Governance program.[10]

The quantifiable benefits from pursuing information governance generally fall into four main categories: optimizing corporate value, risk reduction, hard cost avoidance, and soft cost avoidance. See Appendix D for factors to consider when building a quantitative business case with these ROI categories.

THE SEDONA CONFERENCE PRINCIPLES OF INFORMATION GOVERNANCE

Principle 1. Organizations should consider implementing an Information Governance program to make coordinated decisions about information for the benefit of the overall organization that address information-related requirements and manage risks while optimizing value.

Organizations benefit in several ways from managing information as a valuable asset. In order to realize these benefits, an Information Governance program should be established in a manner consistent with the organization's industry, compliance, and risk environments.

Any Information Governance program should incorporate the following principles: transparency, efficiency, integrity, accountability, and compliance. To be successful, the Information Governance program must be sponsored and firmly supported by the organization's senior leadership.

A core component of any Information Governance program should include a comprehensive data classification capability, combined with the effective, timely deletion of information. By taking a comprehensive approach to identifying and addressing information-related requirements, organizations can ensure compliance needs are met and conflicting issues are considered. It is also helpful to identify and assess information risks, such as user access control (information security) and system failure (business continuity and disaster recovery), and ensure that such risks are understood so effective information controls can be put in place. This approach also aids in understanding information-related strategic and operational objectives to help ensure that information value can be optimized without compliance lapses or uncontrolled risk.

Although there are many stakeholders with divergent interests in managing information, decisions about governing information should benefit the overall organization, rather than a particular department or discipline.

To enable an organization to make coordinated decisions about information for the benefit of the organization, the primary responsibility of an Information Governance

10 *See generally*, S. Soares, *Selling Information Governance to the Business: Best Practices by Industry and Job Function* (2011) (providing insight into the best ways to encourage businesses to implement an information governance program).

program should be to create and maintain processes and procedures necessary for a coordinated, overall approach to decisions about information. If agreement cannot be reached among stakeholders, the Information Governance program should provide a method for decisions to be made (subject to a challenge process) to enable the organization to move forward. Transparency, efficiency, integrity, accountability, and compliance are integral to the ability to perform this overall coordination and tie-breaking function successfully.

Responsible decision makers should use the Information Governance program at the time they make decisions about information. Care should be taken to design the Information Governance program so that it can be used in this way. Existing governance mechanisms (such as budgetary governance or systems approval) may not be designed for users to interface with at the time decisions are being made. However, these can be leveraged or modified or new ones may be created, depending on an organization's circumstances.

Principle 2. An Information Governance program should maintain sufficient independence from any particular department or division to ensure that decisions are made for the benefit of the overall organization.

The information governance function must focus on the best interests of the organization. In order to fairly and effectively balance needs, however, the information governance program should have meaningful and balanced input from such departments as IT, legal, compliance, RIM, and the business units. One approach to accomplish this is to designate an executive who has sufficient independence to balance the competing needs of stakeholders rather than the interests of a single department. Ideally, the executive in charge of the Information Governance program reports at the same level as a General Counsel, CCO, CFO, or CIO. Another way to make decisions for the benefit of the overall organization is through a committee that has representation from impacted stakeholders, coupled with a process for elevating disagreements to a chief executive. Such a structure should be the ultimate goal for organizations with mature Information Governance programs. However, many organizations do not currently have in place any overarching information governance structure and their initial steps may include assigning information governance responsibilities to designated individuals within departments or lines of business. As this is not the optimal governance structure to reap the benefits of a coordinated approach to information governance, organizations should strive for a structure that results in meaningful and balanced input from all impacted departments or divisions as their Information Governance programs mature.[11]

Many organizations have various departments (i.e., business units, IT, Legal, etc.) that take direction from a CEO or COO. Because goals differ across departments or functions, conflicts of interest may arise if the executive responsible for the Information Governance program reports to an individual stakeholder department.

An Information Governance program should ensure that decisions about information are made in the organization's best interests. Deciding for the overall good of the organization involves balancing the sometimes competing interests of many stakeholders. This balancing creates the potential that a given decision may not align with the particular objectives of a given department, particularly when the decision involves a

11 *See* Appendix B for a discussion of the Information Governance Maturity Continuum.

balancing of cost and risk. For example, one stakeholder may believe a cloud-hosted service will reduce the cost of storing information, but another may perceive an increased risk associated with the data being hosted in the cloud. The reduced cost may be attractive to a department such as IT, and the increased risk may be unattractive to another department such as Legal. In many cases, stakeholders can arrive at a mutually agreeable position that maximizes the benefit to the overall organization, for example by implementing mitigation steps that decrease the risk to one department without substantially increasing the cost to other departments.

Though it is appropriate for departments to operate autonomously in carrying out their primary function, decisions about information governance should be coordinated across all departments and stakeholders as they impact the organization as a whole. Because such decisions require an overall balancing between the needs and interests of different stakeholders, it is important for the information governance function to be independent within the organization.[12]

Principle 3. All information stakeholders should participate in an organization's Information Governance program.

Information Governance programs should seek to be inclusive and to involve all parts of an organization (business units, departments, etc.) that have an interest in the company's information.[13] This may require involvement from all of the organization's departments or business units, which may require different levels and types of activity from stakeholders.

An inclusive process will ensure that decisions about information represent all viewpoints, identifying and resolving potential conflicts early and prior to any action being taken that could have an adverse impact to the organization. For example, an organization might consider a policy that bans MP3 (audio) files from being stored on company resources because they are often identified as unauthorized employee music collections, but there may be cases where such files contain training webcasts and may be needed by HR or corporate training. Without involvement of all parties, valuable information could be lost and adversely impact the organization.[14]

However, participation does not require a "seat at the table" for every person or even every department with an interest in the organization's information. In larger organizations, active participation from every group could create an unwieldy team unable to reach decisions. A more effective approach would be to design an appropriate structure or methodology to ensure that all stakeholder interests are represented. An organization could create a process to identify groups with common interests, appoint certain committee members as proxies for other groups, or design surveys or feedback sessions to ensure that all interests are adequately identified and represented.

12 For further explanation, *see* Appendix B.
13 *Cf.* The Sedona Conference, *Finding the Hidden ROI in Information Assets*, February 2011, https://thesedonaconference.org/download-pub/466.
14 *Equal Employment Opportunity Commission v. Ventura Corp. LTD.*, Civ. No. 11-1700, 2013 WL 550550 (D.P.R. Feb. 12, 2013) (finding that even though there was no evidence of bad faith, a company that failed to preserve pertinent emails and hiring-related documents when it migrated to a new software system and restructured its office, ignored repeated requests to preserve the documents, and retained relevant emails that highlighted its missteps in preserving evidence amounted to spoliation that permitted sanction, exclusion of evidence, and an adverse inference instruction).

In most organizations, stakeholders from the core disciplines of records and information management, data privacy, information security, data governance and e-discovery should be represented in the Information Governance program. These disciplines will involve IT, Legal/Compliance, Risk, Audit and RIM functions. Representatives of lines of business and core operational functions should also be included to ensure that the practical needs of the organization are properly considered. It is important to include core operational functions that have unique information governance issues. For example, human resources and environmental functions typically have legally mandated retention for some of their information.

Principle 4. The strategic objectives of an organization's Information Governance program should be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities.

An effective Information Governance program should be designed, implemented, and monitored based upon organization-wide objectives established from a comprehensive assessment of the interests and concerns of key stakeholders within the organization, such as IT, Legal, Compliance, Records and Information Management, and various business units. The program objectives should address and coordinate the stakeholders' existing practices and approaches to issues such as records and information management, privacy and data security, and litigation preservation; and reconcile the practices and approaches with applicable legal requirements. Other major responsibilities of the Information Governance program should include gathering stakeholder requirements, such as those needed to create and publish requirements. Although the Information Governance program does not own the requirements, it owns responsibility for collecting requirements and considering them to arrive at a decision for the good of the organization overall.

To determine its information-related practices, requirements, risks, and opportunities, an organization should first identify the various types of information in its possession, custody or control, assess whether it owns the information or possesses it for third-parties; and determine whether the information is held by the organization, by third-parties for the organization, or both. The organization should next identify its current information lifecycle practices, including practices pertaining to:

- Creation and/or receipt of information;
- Determining location and media for storing information, including in both active and inactive environments;
- Disaster recovery and business continuity;
- Security for private or confidential information;
- Retention of information in both active and inactive environments;
- Implementation, maintenance and release of legal holds due to litigation or government proceedings; and
- Disposal/destruction of information.

A review of existing written policies, procedures, retention schedules, data maps and contractual arrangements is helpful in identifying and understanding these information-related practices. However, input from the organization's information stakeholders, including IT, Legal, Compliance, Records and Information Management, and business units, among others, is also essential to gaining an accurate and complete understanding of both the strengths of current information governance practices and areas where improvement may be necessary.

Organizations can then assess their identified information types and related practices in light of information opportunities, risks and compliance requirements including:

Opportunities

- Reducing costs and risks of complying with e-discovery obligations, by decreasing the volume of unnecessary information, understanding where information is stored, and considering e-discovery costs and risks when approving locations or formats for creating or storing information;
- Utilizing information to support evidence-based decision making;
- Optimizing accessibility of information to enhance productivity and efficiency;
- Realizing cost savings by decreasing the volume of unnecessary information, and rationalizing storage options to better meet demands while reducing cost;
- Enabling access to information for new and valuable combinations and uses;
- Enhancing the organization's reputation as a trusted custodian of PHI, PII, and other classes of protected information; and
- Achieving cost savings and reducing risk through efficient and appropriately-scoped preservation of information for litigation or government proceedings.

Risks

- Loss of records or other valuable information;
- Loss of integrity, authenticity, and reliability of records or other valuable information;
- Unavailability of information vital to the organization's continued operation;
- Accumulation of information (both by the organization and third parties) not (i.e., never or no longer) required for legal compliance or business needs;
- Creation or storage of information in locations or formats that increase the risk or cost of e-discovery, without a corresponding business benefit to outweigh the increased risks and costs;

- Creation of internal RIM requirements that are not followed;
- Breach of PHI, PII, or other classes of protected information;
- Harm to information from malicious access or attack;
- Inability or failure to detect and respond effectively to data breaches;
- Loss of intellectual property protection;
- Loss of privilege or confidentiality of information;
- Failure to preserve information relevant to litigation or government proceedings;
- Over-preservation of information for litigation or government proceedings; and
- Failure to release information (held by the business, by the legal department, or by outside vendors like law firms, expert witnesses, review vendors, etc.), from preservation once no longer relevant to litigation or government proceedings.

Compliance Requirements

- Legal and contractual requirements for:
    - Records creation, retention, management, and disposition;
    - Privacy and security for PHI, PII, and other classes of protected information;
    - Protection of intellectual property and confidential information; and
    - Preserving information relevant to litigation or government proceedings.

These considerations will differ between jurisdictions, industry sectors, and organizations; and among organizations, there will be a range of risk tolerances and cultures regarding these matters. Industry standards, maturity models, and benchmarking data for comparable organizations are useful considerations for this assessment.[15]

15 Useful standards and models include:
- International Organization for Standardization, *Information and Documentation-Management Systems for Records - Fundamentals and Vocabulary,* ISO 30300:2011 (2011).
- International Organization for Standardization, *Information and Documentation - Records Management - Parts 1 and 2,* ISO 15489-1:2001(2001); ISO 15489-2:2001 (2001).
- International Organization for Standardization, *Information Technology - Security Techniques,* ISO/IEC 27000:2012(2012); ISO/IEC 27010:2012 (2013); ISO/IEC TR 27019:2013 (2013).
- ARMA, *Generally Accepted Recordkeeping Principles®* & *Information Governance Maturity Model*, http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles (2013).
- COBIT 5, *A Business Framework for the Governance and Management of Enterprise IT* (2012), *available at* http://www.isaca.org/COBIT/Pages/default.aspx.
- The Sedona Conference, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (Second Edition) (June 2007), https://thesedonaconference.org/download-pub/81.
- ISO standards, such as the ISO 30300 Series, *Management Systems for Records*; ISO 15489, *Records* Management; and the ISO 27000 Series, Code of Practice for Information Security Management.
- ARMA's *Generally Accepted Recordkeeping Principles®* & *Information Governance Maturity Model.*
- COBIT 5, *A Business Framework for the Governance and Management of Enterprise IT.*

An organization should use the results of the above assessment to determine its objectives for information governance. Well-framed strategic objectives for information governance can guide the design and implementation of the organization's Information Governance program, helping to clarify what elements of structure, direction, resources, and accountability will be pursued, as discussed under Principle 5. Establishing strategic objectives in this manner should clarify decision making on priorities and funding of the effort. Strategic objectives should be measurable to better ensure that progress toward them can be observed and reported. Such measures may be quantitative (i.e., data volumes or run-rates) or qualitative (i.e., assessment or audit against program standards or upon completion of transactions or litigation matters). Measurability of objectives is essential for accountability, discussed under Principle 5. Perhaps the most important feature of this exercise is that it compels organizations to look beyond the confines of traditional silos within organizations.[16]

Principle 5. An Information Governance program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.

To provide reasonable assurance that an Information Governance program will meet an organization's strategic objectives, the program should have structure, direction, resources, and accountability. Depending on the size of the organization, responsibilities such as change management and communication to raise awareness of the information governance function, user training, creating the information governance matrix, and gathering metrics required for management control and monitoring may also be important.

Structure

One means of ensuring that an organization's various information needs are comprehensively addressed is to establish a unified framework in which the organization's various information types can be categorized according to information-related compliance requirements and risk controls. Such a framework should categorize information types by content and context.[17] This will normally require input from a wide range of subject matter experts, including, for example, human resources, accounting, compliance, and environmental.

16 For example, in its information governance assessment, a financial services organization confirms that it has customer information subject to privacy and data security requirements, which it regularly transfers to the custody of various service providers in the ordinary operation of its business. From the siloed perspective of privacy and data security compliance, the organization satisfies the applicable requirements of the Federal Trade Commission's Safeguards Rule (FTC Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2002)) by, *inter alia*, establishing internal controls for selecting and retaining service providers and by contractually requiring them to establish safeguards to ensure security for protected customer information. The organization also periodically audits its service providers to assess the effectiveness of their information security safeguards.

However, through its information governance assessment, the organization determines that its internal requirements for records retention periods are not followed by its service providers, such that some service providers retain customer information for either a shorter or longer period of time than is required under the organization's records retention schedule. The organization also determines that its legal hold process may not include certain customer information relevant to litigation that is in the custody of various service providers, yet arguably within the "control" of the organization for discovery purposes.

As a result of the assessment, the organization decides that one of its strategic objectives will be to apply information governance controls to customer information possessed by its service providers. This strategic objective will allow the organization to ensure that service providers implement appropriate safeguards to protect customer information, comply with the organization's records retention schedule and be responsive to legal holds that may be imposed upon customer information possessed by service providers.

17 Information context is significant, because different copies or instances of the same information content may be used for different purposes, thereby triggering different compliance requirements and risks. For example, a single contract may simultaneously exist in multiple instances for different purposes, including the original executed hard copy version; the scanned, digitized version that the organization declares as the official record of the contract; disaster recovery backup copies of the digitized contract; reference copies of the contract used for business convenience in various departments; and a preserved version of the contract under legal hold due to pending litigation. In each of these contexts, different compliance requirements and risks apply to the same information content of the contract.

Attached to this framework of information types are the applicable rules the organization applies to the respective information. These rules reflect legal and regulatory requirements for records retention, information management, and information security and protection. The rules reflect the organization's operational needs for how information will be retained, managed, and protected, and also the organization's risk controls. The unified framework allows the organization to identify, understand, and follow the appropriate rules for its information types.

In place of siloed structures governing data security, retention, and preservation, an organization could establish an information governance matrix. An information governance matrix is a classification structure for the organization's information types similar to a traditional records retention schedule or data security grid but which integrates all established rules governing the organization's information types. An information governance matrix is thus a repository of integrated rules for information from the organization's perspective as a whole, rather than merely one or more of its siloed functions. An information governance matrix should be designed to meet the needs of various audiences and multiple uses within the organization. It is essential, for all of the Company's business information, that the Company establish and clearly communicate responsibility for complying with the integrated rules included in this governance matrix. Otherwise, "orphan data" can greatly increase the cost and risk of e-discovery.

An organization should strive to establish a common vocabulary for its various information types.[18] A common vocabulary helps ensure information is properly classified, so that the applicable rules for such information types can be identified and followed.

Direction

Organizations should communicate to all information users the organization's expectations for information governance. Vehicles commonly used by organizations to provide such direction include policies, contracts, retention schedules or information governance matrices, procedures and protocols, and guidance and training.

Many organizations have an array of policies that directly or indirectly address information governance topics. Examples include a records-and-information management policy, a communications policy, a computer use policy, an Internet and social media policy, a bring-your-own-device policy, an information security policy, and a legal hold policy. In many organizations, such information-related policies accrete over time, each designed to meet the needs of discrete stakeholders and silos of the organization. They commonly address only limited aspects of information governance and may be in conflict with each other. Organizations should identify all such existing policies, review them for inconsistencies and gaps in coverage, and reconcile them or integrate the majority of these policies into a single information governance policy. Similar to the information governance

18 Whether an organization relies upon traditional structures such as records retention schedules and data security grids or integrates them into an information governance matrix, such structures are commonly organized as taxonomies. A taxonomy is a defined hierarchy with classes and sub-classes forming "trees" of classification. In a taxonomy, it is only possible to move downward into sub-classes, or upward into super classes that subsume all of the classes below. Taxonomies are flat and linear, and therefore limiting. In contrast, ontologies link classes in a non-hierarchical way, forming associations that are non-linear. Thus, the widget purchase order may be associated hierarchically with accounting recordkeeping; but at the same time, it may also be associated with documentation of contract rights and duties, and yet other business functions. Instances of the widget purchase order information may also, simultaneously, be associated with disaster recovery restoration, with information protection issues (due to where versions of the purchase order are located physically or virtually), and with applicable legal holds. The complexity of the digital environment, in which the same information content simultaneously exists in different locations and contexts, triggering different information governance rules, makes ontology a promising perspective for applying information governance to an organization's information.

matrix, an information governance policy expresses in one place all of the organization's policy-level expectations for governance of information.

Contracts with third parties are another means of providing direction for information governance. Organizations commonly allow information to be transferred to or held by third parties, such as service providers for business operations; management, legal, accounting, and technology consultants; data hosting providers; and hard-copy records storage providers. The organization's expectations for information governance should be communicated to such third parties through its contracts with them.[19] For example, engagement letters with law firms should confirm the firm's obligations to protect and preserve information, and also the company's right to require destruction or return of information after the matter or engagement is concluded.

Organizations should also have specific procedures and protocols that provide explicit direction on information creation, receipt, use, dissemination, protection, retention, preservation, and ultimate disposition. Organizations should also establish effective guidance and training regarding information governance, delivered in a way that empowers individuals to make timely, compliant decisions regarding information.[20] Accordingly, training and guidance resources should be tailored to meet the specific needs of recipients and should provide the concrete direction the recipients need to make information-related decisions consistent with the organization's information governance expectations.

Resources

Organizations should provide the people, technology, and implementation resources needed to support their Information Governance program and accomplish the organization's strategic objectives.

People resources include staffing of the management and administrative roles supporting the Information Governance program itself, as discussed above under Principle 3. Staffing should be commensurate with the program's scope and objectives, and roles and responsibilities should be defined. Key points of contact should be identified within the organization, and those in such roles should be accessible and responsive. People resources reflect the focus and engagement of stakeholder representatives, such as from Legal, IT, Compliance, Records and Information Management, other administrative functions, and lines of business. People resources also reflect the recognition that information governance is part of everyone's job responsibilities within the organization.

Technology resources include systems and applications used for creating, using, and storing information, into which should be placed structures and controls for information governance. Technology resources also include systems and applications for managing, tracking, and reporting regarding the Information Governance program itself. Both kinds of technology should be used for the program's scope and objectives. Information governance technology resources should be procured only after requirements for such tools have been defined, consistent with the organization's strategic objectives for

19 In some regulated sectors, contractual control of information protection by such service providers is an explicit legal requirement. For example, HIPAA covered entities must contractually require their business associates to provide compliant security for electronic protected health information (ePHI) created, received, maintained, or transmitted on behalf of the covered entity. 45 C.F.R. § 164.314(a).

20 *Day v. LSI Corp.,* No. CIV 11–186–TUC–CKJ, 2012 WL 6674434 (D. AZ. Dec. 20, 2012) (awarding sanctions for, among other things, failing to follow own document retention policy).

information governance. Organizations should carefully consider whether the contemplated technology can fully achieve the program's desired objectives.

Implementation resources are also needed. These include project management tools and processes to be used as elements of the organization's Information Governance program.

Accountability

The effectiveness of an Information Governance program will turn upon whether the organization establishes accountability for meeting program expectations and for achieving the organization's strategic objectives for information governance. In internal control systems, this atmosphere of accountability is the "control environment."[21] The organization's senior leadership establishes the "tone at the top" regarding strategic objectives, the importance of reaching these objectives, expected standards of conduct, and accountability. In all forms of direction, the visible commitment and support of the organization's senior leadership is crucial.[22]

Management reinforces these expectations, and the related roles, responsibilities, and accountability, across the organization. The Information Governance program should clarify roles and responsibilities, both for information users and also for those managing the Information Governance program.

Information Governance program objectives should be linked to observable and measurable outcomes; and compliance audits or comparable assessments of the program should be conducted on a regular, periodic basis, followed by appropriate corrective actions as needed. Program outcomes should be periodically compared to program objectives, and such outcomes should be tracked by those responsible for the Information Governance program.

The results of such outcome measures and program assessments should be reported periodically to the organization's senior leadership to provide reasonable assurance that the program's objectives are or will be satisfied.

Principle 6. The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.

It is a sound strategic objective of a corporate organization to dispose[23] of information no longer required for compliance, legal hold purposes, or in the ordinary

21 The internal control concept of a control environment is a model that organizations may consider in pursuing information governance, particularly for establishing accountability and managing risks around specific objectives. *See* Committee of Sponsoring Organizations of the Treadway Commission ("COSO"), *Internal Control-Integrated Framework Executive Summary - English*, (2013), http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf ("Internal control is a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.").

22 In some aspects of information governance, senior leadership involvement is legally required. For example, entities subject to the FTC's Red Flags Rule must obtain board-level approval of the initial Identity Theft Program, and must involve the board or senior management in the oversight, development, implementation, and administration of the Program. 16 C.F.R. § 681.1(e)(1) & (2). ISO 30300 provides that "Top management is responsible for setting an organization's direction and communicating priorities to employees and stakeholders."

23 In this Commentary, the term "disposal" will be used narrowly to refer to the final destruction or deletion of information that no longer has any regulatory, statutory, compliance, legal or operational value and is not subject to any retention or preservation requirement. The effective disposal of data should purge all copies of that information from relevant systems so that they are no longer retrievable.

course of business.[24] If there is no legal retention obligation, information should be disposed as soon as the cost and risk of retaining the information is outweighed by the likely business value of retaining the information. This may require a culture shift in some organizations that have developed a "keep it just in case" mentality. Typically, the business value decreases and the cost and risk increase as information ages. Timely disposal of information in a consistent and effective manner provides many benefits, including reduced storage and labor costs,[25] reduced costs and risks of complying with discovery obligations, and an increased ability to retrieve important organizational information. Organizations should therefore consider procedures to achieve the regular destruction of unnecessary information.[26] Organizations should also consider whether information considered private or confidential to third parties should be disposed of within a reasonable amount of time after it ceases to be useful to the organization in order to minimize the risk of disclosure.

While most organizations are familiar with managing paper records (and most retention schedules were drafted with paper in mind), it is important that the organization's retention schedules account for both hard copy and electronic records. For example, record owners may find it difficult to apply the concepts original versus copies to digital information.

The term "hold" is used broadly in this commentary to cover preservation obligations that are independent from routine recordkeeping requirements, such as reasonably-anticipated or active litigation, governmental inquiries, outside audits, or contractual requirements. A hold may take the form of:

- A legal or litigation hold, i.e., the preservation of data for purposes of reasonably anticipated or active litigation or investigations;

- A tax hold, i.e., the preservation of information in ongoing audit or review of records related to tax obligations, such as financial and accounting records;

- A contractual hold is an agreed-upon obligation that an organization has with its customers, vendors, divested entities or other third parties that creates an obligation to preserve or dispose of information that exists separately from the retention schedule.[27]

Records Retention

To create a proper data disposal process, the organization should consider all applicable legal, regulatory, and contractual requirements, in conjunction with the business

24 *Managed Care Solutions, Inc. v. Essent Healthcare*, 736 F. Supp.2d 1317, 1326 (S.D.Fla. Aug. 23, 2010) (rejecting the argument that there is no reasonable business routine demanding that data be destroyed after [13 months], especially in light of developments in the technology field (including the ability to inexpensively maintain documents at an off-site server) and industry standards stating the exact contrary." (citing *Matya v. Dexter Corp.*, No. 97-cv-763C, 2006 WL 931870, at *11 (W.D. N.Y. Apr. 11, 2006) and *Floeter v. City of Orlando*, No. 6:05-CV-400-Orl-22KRS, 2007 WL 486633, at * 7 (M.D. Fla. Feb. 9, 2007)).

25 Though some may view data storage as a low-cost concern, the maintenance, retention and discovery-based review of unnecessary information is far from cheap. In the aggregate, storage is quite expensive. *See*, *e.g.*, Jake Frazier, *'Hoarders': The Corporate Data Edition,* LAW TECHNOLOGY NEWS, (2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202581938140.

26 Principle of Disposition, ARMA, *Generally Accepted Recordkeeping Principles*®, http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles (last visited Dec.3, 2013) ("An organization shall provide secure and appropriate disposition for records and information that are no longer required to be maintained by applicable laws and the organization's policies.").

27 An organization should be wary of this type of obligation, as it could create onerous obligations to dispose of copies of electronic data that may not be within the control of the organization, and inconsistent obligations where different contracts prescribe different retention periods.

value of the organization's information. The organization might begin this process by evaluating its legal/regulatory requirements at all levels and across all jurisdictions relevant to its business (state, federal and/or international) and clustering those records into categories.[28] This exercise will enable the organization to more easily identify the appropriate retention period applicable to each category of records, while also facilitating the analysis of certain key factors relevant to the retention determination, including the cost vs. risk associated with a category of records.[29]

It is important for the organization to remember that the operational value of a records category cannot be the sole consideration in determining a proper retention schedule; legal, regulatory and compliance objectives are of paramount concern. It is equally important, however, that operational value (e.g., maintenance of historical records, research and development processes, other business-driven objectives) be considered as the organization formulates its retention protocols. Otherwise, the organization may squander valuable opportunities to reduce cost while minimizing risk. For example, organizations should strive to avoid retaining information simply because it may possibly be useful at some point in the future and instead undertake a cost-benefit and a risk-benefit analysis with respect to each category of data it maintains, thereby ensuring that the advantages of retaining a given set of information outweigh the potential costs and risks associated with disposing of that information.

Hold/Preservation Analysis

Before the organization disposes of any business records, it should conduct a hold analysis to determine whether there are any legal/regulatory or other obligations in place that require the organization to retain information, regardless of its business value. In order to effectively identify its preservation obligations, it is advisable for the organization to develop and implement protocols designed to track legal/regulatory holds and map them to the relevant sources of information, or take other steps to label, segregate and preserve the information. A key aspect of this exercise is to communicate those protocols to the relevant individuals within the organization, and provide a point of contact (typically, a member of the legal or compliance department) who will address any questions regarding hold procedures and best practices.[30]

It is important for the relevant constituencies within the organization – not just the legal/compliance department – to understand that a legal hold supersedes all other records and information management and retention schedules, and that a hold requires the immediate suspension of the disposal process for all affected information during the time mandated by the hold. Thus, it is critical for the organization to incorporate a "hold and release" capability into its records disposition process, so that once the hold is released or has expired, the affected information can be placed back into the appropriate retention schedule.

---

28 For some organizations, local, municipal and/or regional recordkeeping regulations may apply and, if so, should also be considered when developing an appropriate records retention schedule.

29 For more information, *see* ARMA International Standards and Best Practices, http://www.arma.org/r2/standards-amp-best-practices (last visited Dec.3, 2013) as well as the ARMA's Generally Accepted Recordkeeping Principles: Principle of Disposition, http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles (last visited Dec. 3, 2013).

30 For further information on legal holds, *see The Sedona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010), https://thesedonaconference.org/download-pub/470.

Disposition

Once the organization verifies that no legal, regulatory, or operational requirements apply to the information, disposition decisions can be made. In some circumstances, an organization may be able to determine from readily available information whether a record retention or legal preservation requirement applies. In other circumstances, a more detailed investigation and analysis may be required. The analytical approach to such situations is beyond the scope of this Commentary and is discussed more fully in the Sedona publication entitled, "*The Sedona Conference Commentary on Inactive Information Sources*."[31]

Principle 7. When information governance decisions require an organization to reconcile conflicting laws or obligations, the organization should act in good faith and give due respect to considerations such as privacy, data protection, security, records and information management, risk management, and sound business practices.

Organizations often confront conflicting laws or obligations that apply to the same information, particularly when the organization conducts business across numerous jurisdictions.[32] A common example involves the tension between the European Union Data Protection Directive, which prohibits transferring "personal information," and United States federal court jurisprudence that mandates the production of such information during the discovery process.[33] In other circumstances, an organization may be required to preserve certain information for a specified period of time, while another jurisdiction may require such information be destroyed upon the owner's request.

When faced with information governance decisions triggered by such conflicts, the organization's key objective should be good faith compliance with all laws and obligations. Due deference should be afforded to conflicting laws or obligations, particularly when the conflict arises out of interests that span different jurisdictions.[34] Further, the most significant legal/regulatory and business considerations should be prioritized; not all conflicts are capable of complete resolution, and the organization will ultimately need to balance the competing needs, demands, and viewpoints of the stakeholders involved. To the extent compliance with all laws and obligations is not possible or practical; the organization should thoroughly document its efforts to reconcile the conflict and its resulting decision-making process.

---

31 *See*, *The Sedona Conference Commentary on Inactive Information Sources*, (2009) https://thesedonaconference.org/download-pub/64.

32 *Devon Robotics v. DeViedma*, Civil Action No. 09-cv-3552 2010 WL 3985877 (E.D. Pa. Oct. 8, 2010). The plaintiff in a breach of fiduciary duty and tortious interference requested all ESI relating to the former employee defendant, his Italian employer (a rival), and the alleged breach of contract between the plaintiff and the defendant's new employer. The defendant moved for a protective order regarding the production of "documents owned by his employer," arguing that the disclosure was prohibited by the Italian Personal Data Protection Code. The court found that the defendant did not show good cause for a protective order and denied the motion, writing that the defendant "made nothing but a blanket assertion that any disclosure could violate Italian law." The court also stressed the importance of the requested ESI to the plaintiff's claims and the comity factors outlined in *Societe Nationale* (482 U.S. 522 (1987)) weighed in favor of disclosure.

33 *See, e.g. Heraeus Kulzer, GmbH v. Biomet, Inc.*, 633 F.3d 591 (7th Cir. 2011).

34 For example, with respect to the transfer of information from France to the U.S. for use in legal proceedings, which allegedly would have violated a French blocking statute, the U.S. Supreme Court held that U.S. courts should "take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state." *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522, 546 (1987). In so doing, "the concept of international comity requires in this context a … particularized analysis of the respective interests of the foreign nation and the requesting nation." Id. at 543-44.

Principle 8. If an organization has acted in good faith in its attempt to reconcile conflicting laws and obligations, a court or other authority reviewing the organization's actions should do so under a standard of reasonableness according to the circumstances at the time such actions were taken.

An organization's actions may be subject to review by a court or other governing authority regarding its attempt at resolving conflicting laws and obligations. That review should consider the specific circumstances when the information governance decision under review was made. Any judgment of the correctness of past actions to resolve conflicts should be based solely upon what was known at the time the decisions were made. Where a party has acted in good faith, it would be patently unfair to consider what they might have known had they possessed superior prescience.[35]

Application of the reasonableness standards requires that a court or other authority objectively assess the organization's actions or decisions in comparison to the actions or decisions made by a hypothetical, similarly-situated organization acting reasonably under the same circumstances. In *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104 (8th Cir. 1988), the court outlined factors to be considered in assessing the reasonableness of a record retention policy for a spoliation instruction, including: (i) whether the policy was reasonable considering the facts and circumstances surrounding the relevant documents (i.e., whether a three year retention policy is reasonable for a class of materials, such as email); (ii) whether any lawsuits relating to the documents had been filed, or may have been expected; and (iii) whether the document retention policy was instituted in bad faith. *Id.* at 1112.

In determining good faith, courts or other authorities should give due deference to decisions by corporate officers or directors by applying the "business judgment rule," which is a presumption that a business decision was made "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." *Aronson v. Lewis*, 473 A.2d 805, 812 (Del. 1984) (citations omitted).

Principle 9. An organization should consider reasonable measures to maintain the integrity and availability of long-term information assets throughout their intended useful life.

If the intended useful life of an information asset is long enough that risks or concerns may arise regarding the ongoing integrity and availability of the information, then organizations should consider appropriate measures designed to protect those information assets. Therefore, *long-term* planning for availability and integrity depends on the circumstances involved, including the asset's purpose and storage media options.

For example, if your intended retention period is 25 years and the media format you will be using has an expected life of 12 years, then specific planning will be required to

35 *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection*; Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation (European Union Edition), (2011), https://thesedonaconference.org/download-pub/495. Principle 2: "Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness." *See also*, ABA Resolution 103 (2012) (adopted), http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/ resolutions/2012_hod_midyear_meeting_103.doc. 26k-2012-11-10: "t[T]he American Bar Association urges that, where possible in the context of the proceedings before them, U.S. federal, state, territorial, tribal and local courts consider and respect, as appropriate, the data protection and privacy laws of any applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation."

ensure the ongoing integrity and availability of that information. Failing to ensure the integrity and availability of information assets may bring the risk of sanctions if an organization is unable to fulfill e-discovery obligations.[36]

This principle is limited to "systems of record", meaning that copies (such as convenience copies) are outside its scope. Backup and recovery, disaster recovery, and redundant storage paradigms such as 'RAID' are well-understood disciplines dictated by operational business continuity requirements and are therefore not covered by this Commentary. Logical defects prior to "long-term" storage also are not covered by this principle or Commentary.

Long Term Digital Assets

The phrase "long-term" is used to mean a time-frame sufficiently long to involve planning for concerns such as the physical degradation of the storage medium or the impact of changing technologies.

Planning for the ongoing integrity and availability of long-term information assets is important for both physical and digital information, but it is important for digital assets that may have a long lifecycle or retention period. The risks and considerations should be evaluated as part of the long-term retention strategy.

To maximize the probability of ensuring the ongoing integrity and availability of digital assets throughout their intended useful life, organizations should make a good-faith attempt to balance risk and cost. Creating a long-term retention strategy appropriate to the value and type of the information involves considering a broad range of factors pertaining to the digital assets and the circumstances of the organization itself. These factors should include business value, regulatory importance, intended retention schedule, legal hold status, file format, continued availability of the technologies required to access and read, the likely failure rate of the storage medium as it is configured, the available budget and resources of the organization, and/or (for 3rd party services such as *cloud* storage, SaaS, etc.), the contractual agreements between the customer and provider.[37]

Principle 10. An organization should consider leveraging the power of new technologies in its Information Governance program.

For many organizations, reliance on end-users to effectively manage information continues to work well. These organizations should consider how technology can help individuals to better manage the information that they are responsible for, and to monitor management of the information. Examples of the former include limitations on the size of email accounts, or systems that automatically delete emails unless they are moved from the inbox or sent box. Appropriate use of this technology can significantly decrease the cost and risk of e-discovery because emails frequently make up a significant percentage of information that is collected for litigation or government investigations. Similarly, organizations should consider using technology that automatically deletes voicemails after a fixed number of days. Companies can also monitor for over-retention by providing management with lists of the largest email accounts or reports on data that has not been accessed recently.

36 *United States v. Universal Health Servs., Inc.*, No. 1:07cv000054, 2011 WL 3426046 (W.D. Va. Aug. 5, 2011).
37 For a more detailed explanation of the specific areas of risk for digital assets, *see* Appendix C.

However, organizations should consider using advanced tools and technologies to perform various types of categorization and classification activities. While the rapid advances in technology threaten to render obsolete the technology described in this commentary, an organization should consider using technologies such as machine learning, auto-categorization, and predictive analytics to perform multiple purposes, including: (i) optimizing the governance of information for traditional RIM; (ii) providing more efficient and more efficacious means of accessing information for e-discovery, compliance, and open records laws; and (iii) advancing sophisticated business intelligence across the enterprise.

Machine Learning, Auto-Categorization, and Predictive Analytics Defined

Machine learning is the "[f]ield of study that gives computers the ability to learn without being explicitly programmed."[38] Training filters to recognize spam email is one common example of machine learning. In theory, just about any classification problem arising in information governance can benefit from being modeled by machine learning techniques. Some of these techniques do not rely on human intervention: for example, clustering or auto categorizing data into data types or classifications can be accomplished through software alone analyzing the properties of a data set.

One machine learning technique of particular utility involves active learning by software through human interaction on the front end, where humans train the systems to learn through examples. "Predictive coding" and "technology-assisted review" are terms used in the e-discovery arena that rely on humans coding seed sets of data into responsive and nonresponsive categories, with software then analyzing the remaining huge repositories of data.[39] As used here, "predictive analytics" means any machine learning technique that combines human intervention on the front end with the power of machine learning, to optimize the classification of information through automated rules.

New Technologies Meet Traditional RIM

If the structure or volume of information flowing through networks does not allow continued reliance on "end-users" to categorize content, organizations should consider taking steps that shift the burden of traditional records and information management from individuals to technology through auto-categorization of content. Organizations should, therefore, consider taking steps that shift the burden of traditional records and information management from individuals to technology through auto-categorization of content. For example, organizations may use existing software to analyze and categorize the contents of email for purposes of defensible deletion of transitory, non-substantive or non-record content.[40] Organizations increasingly utilize predictive analytics to assist in categorization functions, where individuals train software to differentiate between types of records.

For e-discovery, the first judicial opinions approving the use of predictive coding and technology-assisted review techniques for document review in e-discovery were published in 2012.[41] In one case, the court stated that "the Bar should take away from this

38 Arthur L. Samuel, *"Studies in Machine Learning Using the Game of Checkers,"* IBM JOURNAL OF RESEARCH AND DEVELOPMENT 3(3):211-229 (1959).

39 *See generally*, The Grossman-Cormack Glossary of Technology Assisted Review, 7 FED. CTS. L. REV. 1 (2013).

40 The National Archives and Records Administration has endorsed the use of email archiving and capture technologies using smart filters to sort content through role-based and rule-based architectures. *See* NARA Bulletin 2013-02, *Guidance on a New Approach to Managing Email Records*, (Aug. 29, 2013), http://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

41 *See, e.g.*, *Da Silva Moore v. Publicis Groupe*, 287 F.R.D. 182 (S.D.N.Y. 2012), *approved and adopted in Da Silva Moore v. Publicis Groupe*, No. 11 Civ. 1279(ALC)(AJP), 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012); *Global Aerospace Inc., et al. v. Landow Aviation, L.P., et al.,* No. CL 61040, 2012 WL 1431215 (Va. Cir. Ct. Apr. 23, 2012); *In re Actos (Pioglitazone) Products,* No. 6-11-md-2299, 2012 WL 3899669 (W.D. La. July 27, 2012).

Opinion ... that computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review."[42] An important study by the Rand Corporation, anticipating this new direction in the law, concluded that predictive coding may significantly reduce e-discovery costs by reducing the number of documents requiring eyes-on review.[43]

Predictive Analytics and Compliance

Predictive analytics is also increasingly being utilized by organizations outside of the e-discovery context, including in investigations and as an element of compliance programs. Predictive analytics is being used in compliance programs to predict and prevent wrongful or negligent conduct that might result in data breach or loss. Similar to how this technology is being used in litigation and investigations, predictive analytics is being used as an early warning system. To this end, companies use exemplar documents, sometimes in conjunction with search terms, to periodically search a target corpus of documents, usually email, to detect improper conduct.

Predictive Analytics and Business Intelligence

At its most fundamental level, predictive analytics assists in identifying information that may help to answer a question. There is no limit to the questions predictive analytics can help answer. Companies are beginning to use predictive analytics to develop business intelligence about the company, its information assets, and the market in which it operates.

Principle 11. An organization should periodically review and update its Information Governance program to ensure that it continues to meet the organization's needs as they evolve.

Organizations and their environments change. The footprint and nature of the organization's operations may expand, contract, or transform, and its technology capabilities and uses will evolve. The organization's environment will also change, including legal requirements for the retention, protection, preservation, and disposal of information. And new information-related risks will also arise as time passes. Review of at least some aspects of many organizations' Information Governance programs is legally required,[44] and regardless, is prudent given the inevitability of organizational and environmental change. Organizations, therefore, should periodically review and update their Information Governance program.

42 *Da Silva Moore,* 287 F.R.D. at 193.

43 N. Pace & L. Zakaras, *"Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery,"* RAND Report (2012), http://www.rand.org/pubs/monographs/MG1208.html.

44 For example, HIPAA policies and procedures must be reviewed periodically and updated as needed in response to environmental or operational changes affecting the security of electronic protected health information. 45 C.F.R. § 164.316(b)(2)(iii). HIPAA security measures must also be reviewed and modified as needed to continue providing reasonable and appropriate protection for ePHI. 45 C.F.R. § 164.306(e). Comprehensive information security programs for customer information under the Gramm-Leach-Bliley Act must be evaluated and adjusted in light of any material changes in operations or business arrangements. 16 C.F.R. § 314.4(e). Entities subject to the FTC's Red Flags Rule must ensure that their mandated Identity Theft Program is updated periodically to reflect changes in risks to customers or to their safety and soundness regarding identity theft. 16 C.F.R. § 681.1(d)(2)(iii). And entities that own or license personal information about Massachusetts' residents must review their information security measures at least annually or whenever a material change in business practices reasonably implicates the security or integrity of records containing such personal information. 201 CMR. 17.03(2)(i).

Program review differs from the monitoring activities that should be embedded in the organization's Information Governance program. Such monitoring activities observe whether information-related practices comply with the program's rules and risk controls. *See* Principle 5, Accountability. The program review should seek to determine whether the program itself, and its rules and risk controls, remain appropriate for governing the organization's information in light of organizational and environmental changes. A flawlessly-executed Information Governance program will still result in compliance and risk exposures if elements of the program have become obsolete due to changed circumstances.

The review of the Information Governance program is akin to the assessment described under Principle 4. The organization should:

- identify any significant changes in its life cycle practices for information;
- identify significant changes in applicable compliance requirements and risks regarding its information;
- review the organization's strategic objectives for information governance in light of internal or external changes; and
- review the results from monitoring and measuring performance of the organization's Information Governance program, as an indicator of whether the program's rules and risk controls are adequate or should be refined.

Those responsible for administering the organization's Information Governance program should be involved in the program review. The need for objectivity in conducting such a review may make it valuable to have an independent review of the program. And ultimately, because senior leadership is responsible for the results of information governance at the organization, such senior leadership should participate appropriately in the review process, receive the results of the review, and then provide direction, support, and resources for needed changes in the program.

No bright-line rule governs how frequently an Information Governance program should be reviewed. As with other business-driven initiatives, the frequency of review will most likely depend on many factors relating to the organization.[45] If an organization is rapidly changing through frequent acquisitions and divestitures, or periodically undergoes major updates to its technology systems, then its information environment is likely to be ever-changing to adapt to its new structure or systems. Alternatively, if an organization is relatively mature, has a stable operations model, or is not governed by frequently changing governmental regulations, it may be reasonable for it to conduct its reviews less frequently (i.e., biannually), to reassess and identify potential modifications to its recordkeeping, data security, and operational requirements. Further, an organization may be subject to external pressures, such as regulations subject to frequent modification or regular compliance audits that require systemic changes; in such cases, the organization should be prepared to review and revise its information governance policies on an ongoing basis to meet the challenges posed by such changes. An organization should track pending legislation and regulations

45 Determining the appropriate frequency of review is a matter of business judgment. Courts generally defer to decisions by corporate officers and directors pursuant to the "business judgment rule," which is built upon the presumption that business decisions are made "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." *Aronson v. Lewis*, 473 A.2d 805, 812 (Del. 1984), (*overruled on other grounds by Brehm v. Eisner*, 746 A.2d 244 (Del. 2000).

relevant to its industry to facilitate continued compliance with the regulations that affect its operations. It would be prudent to include a review of its information governance policies and procedures as part of its response to such developments.

Because of the ongoing program review, update, and execution, an organization will have reasonable assurance its Information Governance program continues to meet both legal requirements and also the organization's strategic objectives for information.

APPENDIX A

Intersections

Intersections Create Opportunities and Challenges

Although the functional areas of RIM, E-Discovery, Privacy and Information Security are frequently separate, a successful Information Governance program requires them to work together. As there is some natural overlap between the three groups, some of this will come naturally and provides opportunities to combine resources and budgets. Conversely, in some areas the goals of intersecting groups may clash and require resolution before an initiative can move forward. Identifying and leveraging these areas early in a program is an important task. The table below defines many of the synergies and conflicts in the intersections of these groups.

Functional Area Focus	RIM Intersection with Functional Area	E-Discovery Intersection with Fuctional Area	Privacy Intersection with Fuctional Area	Security Intersection with Fuctional Area
RIM ***Primary Focus:*** *RIM programs ensure that records and information are properly maintained, accessed, and ultimately disposed of in accordance with statutory and regulatory requirements and with consumer expectations. They also ensure that those organizations with which there is a third-party relationship endorse the same safeguards and have appropriate means of guaranteeing compliance.*	**N/A**	**Potential Synergy:** • Similar metadata concerns. • Work together to respond to document requests by locating and preserving relevant information. • Support consistent defensible disposition of information in accordance with an organization's legal, regulatory and operational requirements. • Enables organization to know what they have and identify, preserve, retrieve, search, produce and appropriately destroy in normal course of business. • RIM protects against loss of content that could lead to sanctions, financial loss and brand risk during e-discovery. • RIM serves as evidence of official policy and helps ensure that evidence can be authenticated. **Potential Friction:** • Could be responsible for retention of drafts or outdated content due to relevancy. • RIM focus is can be more narrowly targeted to "records" while e-discovery is broadly on ESI	**Potential Synergy:** • Defines requirements for identification and classification of sensitive information. **Potential Friction:** • RIM may need wide access and distribution while Privacy seeks limits.	**Potential Synergy:** • Ensures that sensitive information is properly maintained, identified and content is classified. • Ensures that sensitive data and information is properly maintained, accessed and disposed of according to legal and regulatory requirements. **Potential Friction:** • RIM may need wide access and distribution while Security seeks limits. • Encryption may be required in Security but frustrate accessibility by RIM.

Functional Area Focus	RIM Intersection with Functional Area	E-Discovery Intersection with Fuctional Area	Privacy Intersection with Fuctional Area	Security Intersection with Fuctional Area
E-Discovery ***Primary Focus:*** *Preservation of electronically stored information that is potentially relevant to impending or ongoing litigation and is processed in a timely, auditable and efficient manner.*	**See RIM / E-Discovery intersection above**	**N/A**	**Potential Synergy:** • Identification at point of creation of information subject to privacy regulations may reduce risk that private information will be produced. **Potential Friction:** • Producing private information protected by another country's laws can result in criminal or civil sanctions. • Refusing to preserve and produce private information may result in civil or criminal penalties under US Law.	**Potential Synergy:** • Ensures that sensitive data and information is available, if relevant; and that out-of-date information is disposed of according to legal and regulatory requirements. • Satisfies an organization's "duty to preserve" for forensic collections. **Potential Friction:** • Security encryption requirements can hamper e-discovery efforts.

Functional Area Focus	RIM Intersection with Functional Area	E-Discovery Intersection with Fuctional Area	Privacy Intersection with Fuctional Area	Security Intersection with Fuctional Area
Security ***Primary Focus:*** *Ensuring the confidentiality, integrity, and availability of information and assets.*	**See RIM/Security intersection above**	**Potential Synergy:** • Ensures that sensitive data and information is available, if relevant, and that out-of-date information is disposed of according to legal and regulatory requirements. • Satisfies an organization's "duty to preserve" for forensic collections. **Potential Friction:** • Security encryption requirements can hamper e-discovery efforts.	**Potential Synergy:** • Security enforces the access rights defined by privacy. **Potential Friction:** • Privacy requirements may hamper security investigations	**N/A**

APPENDIX B

Maturity Continuum as it Relates to Independence

It is important to consider the independence of the Information Governance function of an organization when making determinations such as assessing the current maturity, or planning how to increase the future maturity of an Information Governance program.

While not all organizations have a sufficiently mature Information Governance program to warrant the appointment of a *C* level executive in this role, we believe that organizations must ultimately view information governance as requiring an executive leader that is accountable to the CEO or COO in order to ensure that decisions are made in the best interests of the overall organization, rather than for the good of discrete departments.

A common difficulty when balancing costs and risks occurs when the choices have dissimilar characteristics that make comparison difficult. For example, a clearly-defined cost saving may need to be weighed against a high impact, low-probability event, such as statutory fines in the event of leakage of protected data, where it is difficult to quantify the probability of the event occurring or the costs. Whatever risk management methodology is used to balance cost and risk, it will be more accurate to make the determination by looking at the problem from the perspective of the overall organizational impact.

However, if the executive in charge of information governance reports to an individual department, there is the potential for the interests of that department to be given greater weight than the overall interests of the organization. The simple fact that the department to which the executive reports funds their work and rates their job performance may result in such a bias.

Therefore, the level of independence of the information governance function of an organization is an important component of the information governance maturity continuum.

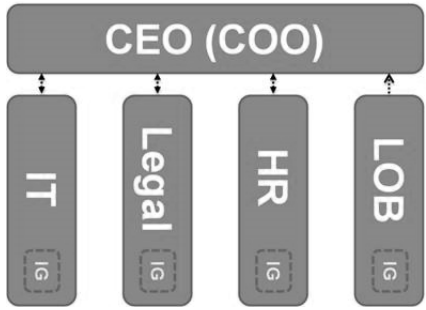
Maturity and Independence

The following discussion is intended as a reference to aid in assessing the current level of maturity of an information function, planning how to move an organization further along the information governance maturity continuum, or making a determination as to what is *sufficient* independence for a given organization. The concepts described below can be adapted for the specific circumstances of an organization.

Note: The following graphics are highly simplified, generic representations of potential organizational structures at varying points along the maturity continuum. The graphics depict the coordination and accountability at a departmental level. Specific functions such as RIM, Privacy, Information Security, E-Discovery, etc. are intentionally not shown because they generally reside within a stakeholder department.

Immature

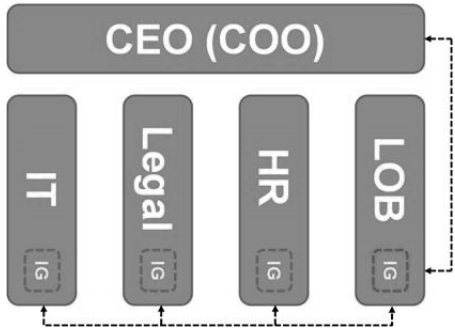
Immaturity is characterized by a lack of over-arching coordination of information governance stakeholders and no single point of accountability to the CEO or COO for overall governance of information**.**



At the immature end of the maturity continuum, lack of coordination creates a potential for important requirements being missed. Decisions and requirements reside in silos, and cross-functional coordination is ad hoc. There is a potential for departmental decisions that conflict with other stakeholder requirements and which are not in the interests of the organization overall. There is also a potential for inconsistent treatment of different items in the same category in the same circumstances.

Less Mature

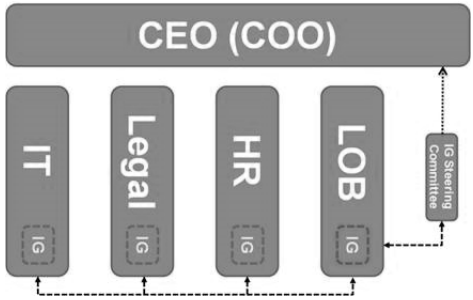
At this area of the maturity continuum, ownership of information governance process resides within a stakeholder department.



There is a potential conflict of interest since ownership must reside in a stakeholder department, which presents the problem of misaligned incentives.

More Mature

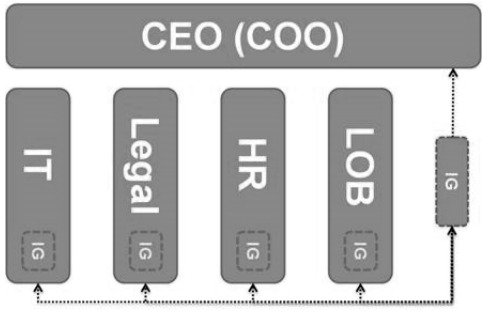
At this area of the maturity continuum, ownership of Information Governance process resides in a stakeholder department but is accountable to a steering committee of *C* level executives from the stakeholder departments who are accountable to the CEO or COO.



There is still a potential for conflict of interest for the executive in charge of Information Governance (who resides in a stakeholder department) and for the *C* level executives on the Information Governance steering committee because the goals of the individual departments may conflict with the goals of the overall Information Governance program.

Mature

A mature Independence Governance function is characterized by an executive who resides in a separate Information Governance department who is accountable to the CEO or COO for coordinating stakeholders across all departments and functions and balancing decisions for the benefit of the organization overall.



APPENDIX C

Risks Associated with Digital Assets

Risks

There are specific areas of risk for digital assets that organizations should consider, including:

Integrity

The term "integrity" is used to mean the authenticity and reliability of the information. In some situations this may simply mean the logical content of the information has not been altered. In other situations it may mean the file can be guaranteed not to have changed.

The integrity of the information, or of information required to access the information (such as an index or necessary metadata) may be compromised by factors such as unauthorized alteration, or degradation of the storage medium. These risks can become particularly acute during platform migration.

Consideration should be given to: (a) the level of integrity required both for the digital asset in question and the technologies required to read and access the data, and (b) the level of difficulty involved in repairing or recovering damaged digital information.

Careful consideration should be given to the file format, storage medium (including the configuration of that storage medium), and the circumstances of operation and storage, in order to ascertain the likelihood of data loss.

Digital storage media without moving parts such as flash drives, solid state drives, and tape, or with rarely moving parts (such as storage devices intended for infrequent use that power off when not in use) still fail. Unused storage media on a shelf (for example, forensic collections on individual storage media in an evidence lab) will eventually become unusable. Given the relatively short lifespan (say, three-to-five years) of some items of storage media, a legal hold or retention requirement that may potentially exceed the reasonably expected lifespan could necessitate specific *long-term* planning due to the failure rate of the technology involved.

Availability

The term "availability" is used to mean "able to be used when needed," which includes:

- any element (such as security mechanisms to protect the data, access rights required to access the data, or applications required to interpret or read the data);
- being able to access information in a timely manner (for example within applicable service-level agreements, contractual requirements, or timeframes indicated by legal requirements);

- being available within a pre-agreed lead-time (depending on business need – for example, a week).

Note that availability does not necessarily mean continuous availability.

The availability of information, or information required to access the information (such as an index or necessary metadata) may be compromised by obsolescence or unavailability of technology required for accessing the information (or index, or necessary metadata) in a timely manner.

Considerations

When planning for ongoing integrity and availability of digital assets throughout their intended useful life, important considerations include:

Technology Refresh Period

The phrase "technology refresh period" is used to refer to the timeframe in which technology components are expected to fail, and within which planning needs to occur for replacing those components.

Organizations should exercise prudence when considering the technology refresh period for long-term digital assets. For example, if the expected lifespan of the storage medium is seven years, then the technology refresh period should be less than seven years. The timing of the technology refresh period compared to the technology's expected lifespan is a matter of risk calibration and business judgment.

Planned Migrations

Obsolescence of technology is a major consideration in long-term storage of digital assets and requires careful planning. Migrations (moving to a new platform for the archive as a whole or for a component of the archive) are a consequence of obsolescence that must be planned. All elements of the archiving system including search-and-retrieval capability as well as storage medium should be considered in terms of obsolescence. Organizations should consider creating an obsolescence review period as part of their long-term archival planning, because unlike a technology refresh period (which can be ascertained in advance for each technology refresh cycle by reference to the expected life of the technology components) the probable time of obsolescence may not be knowable in advance.

Migrations may also require format conversions, and integrity-checking technologies (see below) are particularly critical to ensure the data is not inadvertently changed during a migration.

Matching Storage Medium to the type of Electronic Information

It is important to match the characteristics of the storage medium to the requirements of the information being stored. For example, micrographics work particularly well for text documents – particularly text documents held for reference purposes – but not for binary files such as audio files or CAD (Computer Aided Design) files. Micrographics also may not work well for files that need to be in digital format when used because a scanning or conversion process will be required before the file can be used.

The expected failure rate of the storage medium should be considered in terms of the expected retention period. Regulated utilities or pipelines often involve document retention periods of decades, sometimes over 50 years, often longer than the life of the plant.

Integrity-Checking Technologies

Passive integrity-checking technologies can be used to assess if a file has changed. These technologies include such mechanisms as hash values created by hash algorithms computed when a file is retrieved and if the file has changed. Unfortunately, passive integrity-checking technologies have no inherent mechanism to repair files and restore them to their original form; they can only alert you to the fact that a problem has occurred.

Active integrity-checking technologies can be used not only to assess if a file has changed but also (if appropriately configured) to restore a file to the original form as when it was stored. There are many proprietary examples of integrity-checking archive technologies. Because these technologies are generally well-understood and well documented, they are not discussed further here.

Long Term Physical Information Assets

When considering storage using physical mediums such as paper, it is important to ensure that the expected life of the storage medium exceeds the retention requirements. In the case of printed paper, the expected life of different types of paper, as well as different types of ink, can vary a great deal. It is also important to consider the storage conditions (such as humidity and temperature) required to ensure the ongoing integrity of the physical assets because this can affect the expected life of the physical storage medium.

APPENDIX D

The Quantitative/ROI Business Case

As discussed in the Commentary, a successful information governance approach requires both strategic commitment (adoption as an organizational priority) and tactical efforts. This Appendix discusses approaches to establishing an acceptable ROI for particular projects.

A typical ROI analysis weighs the benefits of a particular project against its cost, and calculates the length of time it will take to recoup the cost. The quantitative aspects of the business case are best determined by focusing on specific applications of information governance to identified problems or opportunities, or to discrete projects for implementation of the Information Governance program.[1]

The quantifiable benefits from pursuing information governance generally fall into four main categories: optimizing corporate value, risk reduction, hard cost avoidance, and soft cost avoidance.

Optimizing Corporate Value

Information governance can help make information assets available for new, valuable uses. It can also allow organizations to derive value from engaging in what might otherwise be cost-prohibitive endeavors, due to efficiencies and cost savings realized through information governance practices. In general, Gartner has identified the following as possible "adds" to corporate value from an Information Governance program:

- **Effectiveness:** Such as due to document-centric collaboration tools;
- **Cost/efficiency:** For example, from imaging/workflow solutions to replace traditional paper-oriented processes;
- **Customer service:** Such as from customer-relationship solutions that lead to better market penetration and customer satisfaction;
- **Competitive advantage:** As more modern tools and reliable information allows for speedier delivery of goods or services to customers; and
- **Revenue:** Such as a result of enhanced social media and web presences and solutions.[2]

> By way of example, a core benefit of an Information Governance program is to ensure that information used for different purposes across the enterprise – e.g., for sales and marketing, but also for planning, billing, fulfillment, financial, customer feedback and other downstream purposes – is reliable or trustworthy, accurate,

1 *See generally*, S. Soares, *Selling Information Governance to the Business: Best Practices by Industry and Job Function* (2011) (providing insight into the best ways to encourage businesses to implement an information governance program).
2 *See* Gartner, *"First 100 Days: Enterprise Content Management Initiatives"* (July 7, 2011), *available at* http://www.gartner.com/id=1739415.

> and in formats usable across platforms or applications. Achieving these objectives requires that IT understand not only the business purposes and objectives but also whether data elements require special protections or treatments (e.g., for legal, RIM, privacy or security reasons).[3] Yet, oftentimes when a large organization initiates such a program, it finds that different business units or functions use different terminology for the same content concept. For example, an organization may refer to outside business partners as *vendors*, *suppliers*, *associates*, or *providers* and collect various information about such entities in systems that support particular functions within the organization. But if the terminology – or application – differs between and among business units, opportunities to cross-sell or otherwise leverage the information about the business partners may be missed.[4] Thus, an early goal for an Information Governance program may be to develop a common vocabulary and understanding of what information-related assets exist; once that is done, the organization may realize that business advantages may be achieved – at virtually no cost – by cross-utilizing existing information or systems.[5]

Mergers and acquisitions, or technology upgrades, also present opportunities (and challenges) for improving data quality and corporate revenues by, for example, merging (and purging) customer lists to identify strong customers across multiple business lines.[6]

Risk Reduction

Risk reduction is also a significant benefit of information governance. Business value may not be realized if an unanticipated risk creates an unexpected cost. For example, organizations may leverage information over the short-term (e.g., email for current communications), but once the information is no longer useful, the ESI is often stored away, rarely accessed, and often never re-assessed to determine whether the benefits of continued retention outweigh the risks. Thus, what was once a business asset may become a source of risk for certain organizational areas such as compliance or e-discovery, while providing little or no benefit for other organizational areas such as business units. Through proper information governance, organizations can recognize these perils and elect to remediate the un- or under-utilized information assets, and optimize the business value of information while managing the associated risks.

Many types of adverse events can be avoided through effective information governance. The value of risk reduction can be estimated by quantifying the potential losses that would result if an adverse event occurred and determining the reduced likelihood of such an occurrence due to effective information governance. Some examples of risks posed by information assets follow:

---

3 *See, e.g.*, Soares, *supra,* at 149.

4 As another example, it has been reported that one manufacturing company discovered and eliminated 37 unique definitions of "customer" across its enterprise, and agreed on a single, standard definition. Robert Routzahn, *"Business and IT Collaboration: Essential for Big Data Information Governance,"* IBM Data Magazine, (July 5, 2013), http://ibmdatamag.com/2013/07/business-and-it-collaboration-essential-for-big-data-information-governance/.

5 *See, e.g., "The Sedona Conference Commentary on Finding the Hidden ROI In Information Assets",* The Sedona Conference, (Feb. 2011), https://thesedonaconference.org/download-pub/466.

6 A medical device manufacturer estimated that improving ship-to addresses in a 100,000 item database could increase aftermarket sales by $1 million. Soares, *supra*, at 69.

a. **Data Leakage:** Many companies have valuable intellectual property that is more likely to be lost or leaked to the public and/or competitors if not properly managed through policies and procedures that emanate from a mature Information Governance program.

b. **Privacy Breaches:** A myriad of regulations applicable to particular sectors in the U.S. (e.g., HIPAA to health information, GLBA to financial institutions, PERPA to federally funded educational institutions) require certain data to be protected and impose fines and other sanctions when the data is not properly protected or is improperly disclosed.

c. **Security Lapses:** Regulations such as the self-regulatory Payment Card Industry Data Security Standards require companies to protect credit card and other payment information, or face fines.

d. **Brand Impact:** A breach of private customer information, such as contact information or social security numbers, can adversely impact a company's brand and result in lost sales and/or consumer goodwill.

e. **Litigation/Regulatory Risk:** Access to the most relevant information at the inception of litigation or a regulatory inquiry may allow for an earlier and more accurate assessment of litigation risk, and thus, permit such events to be more effectively and economically managed.

Hard Cost Avoidance

Many benefits flowing from an information governance initiative are based on the premise that certain future costs can be delayed, reduced or avoided entirely because lesser volumes of data will be kept in a more efficient manner. These benefits can be quantified, and in an information governance initiative, often arise from the following areas:

a. **Storage:** Storage and maintenance costs can be radically reduced by the rationalizing data storage options, eliminating outdated ESI that no longer serves a legitimate business, legal or regulatory purpose, and moving valuable information that is occasionally and non-critically accessed to cheaper storage. A systematic approach to information governance may allow an organization to archive its less active and less critical data on less expensive tiers of storage, which in turn can eliminate unnecessary duplication of documents, associated backup overhead and better enable data disposition in line with organizational policy.

b. **Outdated Backup Media:** Eliminating the retention of large (and outdated) quantities of backup media, such as magnetic tapes, reduces the costs of backup media and related storage, labor and transfer expenses.

c. **Personnel Costs:** A successful Information Governance program will reduce the volume of ESI and make it easier to manage and to find information. Accordingly, fewer personnel would be required to manage the reduced volume, allowing the organization to realign resources appropriately.

d. E-Discovery Costs: A reduced volume of electronic information can, in the event of litigation, reduce litigation costs *significantly*, because there will be less information to process and review.[7]

Soft Cost Avoidance

Other benefits resulting from improved information governance save time and effort that can be deployed for other activities. For example, having a more efficient method for storing and accessing email messages might save 30 minutes per day for each employee, netting a direct financial savings to the organization, or allowing employees to focus on more useful activities. Soft costs are often difficult to quantify, but the following are useful considerations:

a. Economies of Scale: Managing information on an *ad hoc* basis can result in requirements and risks being overlooked, benefits not being realized, and tremendous amounts of inefficiency due to the redundancy of effort this entails. Economies of scale can be realized by having an over-arching Information Governance program at an organizational level, which generates processes and procedures to govern how ESI is handled.

b. Organizational Inefficiencies: Organizations with excessive amounts of uncategorized ESI are often unable to locate needed information in a timely and efficient manner. An Information Governance program that creates an infrastructure for information assets promotes shorter client response times, allows the re-purposing of institutional knowledge, and enhances continuous improvement efforts.

7 A recent Rand survey states that the review process alone averages $18,000 a gigabyte, meaning that with collection, preservation, hosting, etc., e-discovery costs can easily exceed $20,000 a gigabyte. Pace, Nicholas M. and Laura Zakaras. *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*. RAND Corporation, (2012), http://www.rand.org/pubs/monographs/MG1208. Also available in print form.