IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Commentary_on_Information_Governance

wgs

The Sedona Conference

Commentary on Information Governance, Second Edition

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

October 2018
Public Comment Version
Submit comments by December 5, 2018, to
comments@sedonaconference.org

The Sedona Conference
Commentary on Information Governance, Second Edition

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

OCTOBER 2018 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Drafting Team

Michael Burg
Abigail Dodd
Thad Gelsinger
Ronald J. Hedges
Courtney Jones Kieffer
Mollie Nichols
Robb Snow
Joe Treese

Drafting Team Leader

Cheryl Strom

WG1 Editors-in-Chief & Steering Committee Liaisons

Dean Kuckelman
Kevin F. Brady
Heather Kolasinsky

Staff Editor: Susan McClain

We thank all of our Working Group Series 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.

Preface

Welcome to the 2018 Public Comment Version of The Sedona Conference *Commentary on Information Governance*, *Second Edition*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

In 2014, The Sedona Conference published its first edition of the *Commentary on Information Governance* which recommended a top-down, overarching framework guided by the requirements and goals of all stakeholders that enables an organization to make decisions about information for the good of the overall organization and consistent with senior management's strategic directions. This Second Edition of the *Commentary on Information Governance* ("Second Edition") accounts for the changes and advances in technology and law over the past four years; underscores the role of IG as part of and complimentary to the business, rather than something separate that adds overhead; and emphasizes the costs of eDiscovery which should drive organizations to focus on IG on the front end, resulting in eDiscovery that is more efficient, less painful, and which allows the organization to reap additional benefits from a business perspective. Additionally, this Second Edition also incorporates the knowledge and guidance embodied in the new and updated Sedona commentaries since 2014 such as *The Sedona Principles, Third Edition* and The Sedona Conference *Principles and Commentary on Defensible Disposition*.

The Sedona Conference acknowledges the efforts of Drafting Team Leader Cheryl Strom who was invaluable in driving this project forward. We also thank drafting team members Michael Burg, Abigail Dodd, Thad Gelsinger, Ron Hedges, Courtney Kieffer, Molly Nichols, Robb Snow, and Joe Treese for their efforts and commitments in time and attention to this project. Finally, we thank Dean Kuckelman, Kevin Brady, and Heather Kolasinsky who served as both the Editors-in-Chief and WG1 Steering Committee Liaisons to the drafting team.

Please note that this version of The Sedona Conference *Commentary on Information Governance, Second Edition* is open for public comment through December 5, 2018, and suggestions for improvement are very welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please submit comments by email to comments@sedonaconference.org.

In addition, we encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent damages and patent litigation best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it

should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
October 2018

Table of Contents

The Sedona Conference Principles of Information Governance

1. Organizations should consider implementing an Information Governance program to make coordinated, proactive 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 stakeholders' views/needs should be represented 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 data privacy, data protection, data security, records and information management (RIM), 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.

I. INTRODUCTION

Information is one of modern businesses' most important assets. Like any asset, 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, interdisciplinary 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 faced by different information-focused disciplines, such as Records and Information Management (RIM),[1] data privacy,[2] information

---

1 **RIM** 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 a specific 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* Council Directive 95/46/EC of the European Parliament and of the Council 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 O.J. (L 281) 31; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)), Council Regulation 2016/679, 2016 O.J. (L 119) 59, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN ("[A] data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation."). In the United States, 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).

security,[3] and electronic discovery (eDiscovery).[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 guided by the requirements and goals of all 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 the following:

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

---

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 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., Health Insurance Portability and Accountability Act (HIPAA) Security Rule), contract, industry requirements (e.g., Payment Card Industry (PCI)), or company requirements and best practices.

4 **eDiscovery** is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing electronically stored information (ESI) relevant to pending or anticipated litigation or investigation or requested in government inquiries, after the application of any privileges or protections to the ESI.

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

II. 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. An organization's failure to dispose of information that no longer adds value can increase the costs and risks of complying with discovery obligations.[6]

In addition, information control lapses can have significant repercussions, some of which can be highly public:

- Data privacy and security breaches, such as a nationwide credit-reporting agency that compromised sensitive personal information of up to 147 million Americans (about half of the country) in 2017.[7]

- A non-economic impact related to data privacy, such as a major retailer that contacted a frequent customer whose recent purchases suggested that she might be pregnant. When the retailer sent special offers to the "expectant mother" (a teenaged girl), her parents intercepted the mailing and discovered their daughter's pregnancy. The ensuing publicity suffered by the retailer illustrates the potential risk inherent in poor Information Governance controls around a fundamental data mining process.[8]

- 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. Department of Justice for record-keeping violations under the Controlled Substances Act.[9]

---

6 *See The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 60 (2018) ("There is often a direct correlation between an organization's IG program and the ease with which it can search for, identify, and produce information.").

7 Sarah Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could be Affected*, CNN TECH, https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html (Sept. 8, 2017).

8 Hon. John Facciola, Technology and e-Discovery Competence: Enhancing Your Career, Speech to University of Florida Levin School of Law (Oct. 22, 2014), *available at* https://www.youtube.com/watch?v=nNwnBqd_OwY.

9 Press Release, Immigration and Customs Enforcement, Department of Homeland Security, Abercrombie & Fitch Fined after I-9 Audit (Sept. 28, 2010), *available at* https://www.aila.org/File/DownloadEmbeddedFile/51319; Press Release, Drug Enforcement Administration, Department of Justice, CVS to Pay $11 Million to Settle Civil Penalty Claims Involving Violations of Controlled Substances Act (April 3, 2013), *available at* https://www.dea.gov/press-releases/2013/04/03/cvs-pay-11-million-settle-civil-penalty-claims-involving-violations-0.

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.

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

A. 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 Information Technology (IT), Legal, Compliance, RIM, Human Resources (HR), Finance, Data Governance, and the organization's various business units. Each business unit or administrative function commonly has its own goals and priorities, and, accordingly, 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), eDiscovery (focused on preservation and production of information in litigation), and data governance[10] (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, such as the following:

---

[10] 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, 30–33 (2013), *available at* http://jolt.richmond.edu/jolt-archive/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 INST., http://www.datagovernance.com/adg_data_governance_definition/ (last visited Sept. 12, 2018). So viewed, "data governance" does not address "why" an organization chooses to do certain things with its data and other information. The critical role of Information Governance is ensuring that actions that users take with information-related assets are consistent with organizational strategy.

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

- The IT Department enables enterprise information technology platforms absent any consideration of incorporating proper governance.

- 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 the unnecessary retention of data.

- Personnel can 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, controls, or planning for naturally 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 information 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 results in inconsistent application of such requirements to records.

- Records managers initiate 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 eDiscovery 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, which negatively impacts 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.

B. Information Governance

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 do the following:

- Establish a structure for Information Governance, which will vary in form depending on the organization's size, complexity, culture, 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.

- Identify major stakeholders and understand those stakeholders' goals, needs, and concerns.

- Reconcile the various goals, compliance requirements, and risks addressed by different information-focused disciplines, such as RIM, privacy, information security, and eDiscovery.

- 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.

C. 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 organization-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 eDiscovery and responses to audits and investigations and other incidents (i.e., a data breach)

- A framework for defensible disposition

- Better preparedness for new laws and emerging technologies that may introduce other challenges

- More effective risk management

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

- Reduced costs and liability and enhanced compliance with legal obligations for records retention, privacy, data security, and eDiscovery, as information policies and processes are rationalized, integrated, and aligned in accord with the organization's Information Governance strategy

D. 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 through the following:

- 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

- Ensuring that the Information Governance program is administered in a manner 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 but also may become a significant liability. Through proper Information Governance, organizations can realize additional benefit from their information assets over time while reducing risk and costs.

E. 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 as an organizational priority) and 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 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, return on investment (ROI)) elements.

1. 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 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:

- **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 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, ethics, and integrity programs to ensure information-related legal compliance and risk management.

- **Data Privacy and Information Security Benefits**

Organizations need to be concerned about ensuring the security of its information and the privacy of employee and customer data. Information Governance will provide a framework for organizations to ensure the necessary controls are in place to protect and secure its information and reduce the amount of unnecessary information by following consistent defensible disposition practices.

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 organization's fundamental values because information is managed in a way that fits an organization's culture.

Conversely, Information Governance also helps organizations avoid cultural dissonance for their core values, such as the "low cost provider" that squanders money on information inefficiency and unnecessary retention; the "innovative excellence" organization that fails to optimize the value of its information; the "trusted partner/provider" that is careless with the information entrusted to it; or the organization espousing "integrity and ethics" that fails to adopt measures that treat its information as a valuable asset and that 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.

2. The Quantitative/ROI Business Case

A typical ROI analysis weighs the benefits of a project against its cost and calculates the length of time it will take to recoup such 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.[11]

The quantifiable benefits from pursuing Information Governance generally fall into four main categories: optimizing organization 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.

---

11 *See generally* SUNIL SOARES, SELLING INFORMATION GOVERNANCE TO THE BUSINESS: BEST PRACTICES BY INDUSTRY AND JOB FUNCTION (MC Press 2011) (providing insight into the best ways to encourage businesses to implement an Information Governance program).

III. THE SEDONA CONFERENCE PRINCIPLES OF INFORMATION GOVERNANCE AND ASSOCIATED COMMENTARIES

Principle 1: Organizations should consider implementing an Information Governance program to make coordinated, proactive 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. To realize these benefits, it is important that an effective Information Governance program 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, compliance, and accountability. To be successful, the Information Governance program must be sponsored and firmly supported by the organization's senior leadership. Clear and open communication among stakeholders with divergent interests is necessary, as is their willingness to put the good of the organization before the needs of their individual business group.

A core component of any Information Governance program should include a comprehensive data classification capability combined with the effective and timely deletion of appropriate 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 to ensure that such risks are understood so that effective information controls are 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.

To enable an organization to make decisions about information for the benefit of the organization, the primary responsibility of an Information Governance program should be to create and maintain processes and procedures necessary for a coordinated, overall approach. 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.

Responsible decision-makers should use the Information Governance program any time they make decisions about information. Care should be taken to design the Information Governance program so that it can be used regarding existing information and information that will be created. At the time decisions regarding information are being made, existing governance mechanisms (such as budgetary governance or systems approval) may not be designed for the current need of its users. 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. 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, such as a Chief Information Governance Officer, 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 (GC), Chief Compliance Officer (CCO), Chief Financial Officer (CFO), or Chief Information Officer (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.[12]

Many organizations have various departments (i.e., business units, IT, Legal, etc.) that take direction from a Chief Executive Officer (CEO) or Chief Operating Officer (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. This involves balancing the sometimes-competing interests of many stakeholders. This balancing creates the potential that a given decision may not align with the objectives of a given department, particularly when the decision involves a balancing of cost and risk. For example, the IT Department may believe a cloud-hosted service will reduce the cost of storing information, but the Legal Department may perceive an increased risk associated with the data being hosted in the cloud. In many cases, stakeholders can arrive at a mutually agreeable position that maximizes the benefit to the overall organization, such as 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

---

12 *See* Appendix B for a discussion of the Information Governance maturity continuum.

overall balancing between the needs and interests of different stakeholders, it is important for the Information Governance function to be independent within the organization.[13]

Principle 3: All stakeholders' views/needs should be represented in an organization's Information Governance program.

Information Governance programs should seek to be inclusive and to consider the requirements of all parts of an organization (business units, departments, etc.) that have an interest in the storage, retention, and management of an organization's information.[14] This may require involvement from all the organization's departments or business units, requiring different levels of participation from stakeholders.

An inclusive process will ensure that decisions about the management of information represent all viewpoints by identifying and resolving potential conflicts early and prior to any action being taken that could have an adverse impact to the organization. For example, a litigation hold formulated by outside counsel might be revealed as overly broad or costly when presented by the GC in an Information Governance discussion that includes line-of-business stakeholders, the CIO, and other key Information Governance participants.

However, all stakeholders' 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, request requirements documentation from every stakeholder, or design surveys or feedback sessions to ensure that all interests are adequately identified and represented.

In most organizations, stakeholders from the core disciplines of RIM, data privacy, information security, data governance, and eDiscovery 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 consulted to ensure that the practical needs of the organization are properly considered. It is important to include active participation from core operational functions that have unique Information Governance issues. For example, HR, highly-regulated departments, and environmental functions typically have legally mandated retention for some of their information.

---

13 For further explanation, *see* Appendix B.

14 *Cf.* The Sedona Conference, *Commentary on Finding the Hidden ROI in Information Assets*, 13 SEDONA CONF. J. 267 (2012).

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, RIM, and various business units. The program objectives should address and coordinate the stakeholders' existing practices and approaches to issues such as RIM, privacy, data security, and preservation; and must reconcile these practices and approaches with applicable legal requirements and business needs. The key responsibility of a cross-organizational Information Governance forum is to provide the mechanisms that allow decisions about information to include the viewpoints of all stakeholders, in order to recognize conflicts of any significant decision involving the organization's information assets. Another major responsibility of the Information Governance program is understanding stakeholder requirements and priorities. Although the Information Governance program is not ultimately responsible for execution of requirements, it owns responsibility for gathering stakeholder needs and priorities, tracking and identifying issues or conflicts resulting from decisions (including escalation, if required), and considering them to establish requirements that serve 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 on behalf of third parties; and determine whether the information is held by the organization, third parties on behalf of the organization, or both. The organization should next identify its current information lifecycle practices, including practices pertaining to the following:

- Creation and/or receipt of information
- Determination of the location and media for storing information, including in both active and inactive environments
- Disaster recovery and business continuity
- Security for private, protected, or confidential information, such as electronic protected health information ("ePHI"), protected health information ("PHI"), personally identifiable information ("PII"), payment card industry information ("PCI"), social security numbers, and sensitive identifiable human subject research and export-controlled research
- Retention of information in both active and inactive environments

- Disposal/destruction of information, as well as exceptions from the normal data lifecycle (e.g., implementation, maintenance, and release of legal holds due to litigation or government proceedings)

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 stakeholders, including IT, Legal, Compliance, RIM, 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 the following:

1. Opportunities

- Reducing costs and risks of complying with eDiscovery obligations by decreasing the volume of unnecessary information, understanding where information is stored, and considering eDiscovery costs and risks when approving locations or formats for creating or storing information

- Monetizing the value of an organization's data

- Reducing the risk of data breach or leakage by adopting sound, effective information security and storage measures

- Using information to support evidence-based decision-making

- Optimizing storage and 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

- Achieving cost savings and reducing risk through early stakeholder involvement and proactive decision-making regarding storage, retention, and organization of business data

2. 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 legal risk or business cost, without a corresponding business benefit to outweigh the increased risk and cost
- Creation of internal RIM requirements that are not followed
- Breach of ePHI, PHI, PII, PCI, social security numbers, sensitive identifiable human subject research and export-controlled research, 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
- Loss of information resulting from organization mergers and acquisitions (when companies are combined, it is common for the staff with the most knowledge of one organization's data to leave, essentially leaving the combined organization with no way to know what the universe of data is, and where it is stored)
- Failure to preserve information subject to regulatory requirements or relevant to litigation, government proceedings, or internal investigations
- Over-preservation of information subject to regulatory requirements or relevant to litigation, government proceedings, or internal investigations
- Failure to release information back into its normal lifecycle once circumstances requiring an exception (e.g., legal hold) have expired

3. Compliance Requirements

- Legal and contractual requirements may exist for the following:
  - Records creation, retention, management, and disposition
  - Privacy and security for ePHI, PHI, PII, and other classes of protected, private, and confidential information
  - Protection of intellectual property and confidential information
  - Preserving information relevant to litigation, government proceedings, and regulatory requirements

These considerations will differ among jurisdictions, industry sectors, and organizations, and 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]

An organization should use the results of the above assessment to determine its objectives for Information Governance. Well-framed strategic objectives 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

---

[15] Useful standards and models include the following:

- International Organization for Standardization (ISO), Information and Documentation—Management Systems for Records—Fundamentals and Vocabulary (ISO 30300:2011).
- ISO, Information and Documentation—Records Management—Parts 1 and 2 (ISO 15489-1:2001; ISO 15489-2:2001).
- ISO, Information Technology—Security Techniques (ISO/IEC 27000:2012; ISO/IEC 27010:2012; ISO/IEC TR 27019:2013).
- ARMA Int'l, *Generally Accepted Recordkeeping Principles®*, https://cdn.ymaws.com/www.arma.org/resource/resmgr/files/Learn/2017_Generally_Accepted_Reco.pdf (updated 2017).
- ISACA, *A Business Framework for the Governance and Management of Enterprise IT*, http://www.isaca.org/COBIT/Pages/default.aspx (last visited Sept. 12, 2018).
- *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production,* 19 SEDONA CONF. J. 1 (2018).
- ARMA Int'l., *Information Governance Maturity Model*, https://www.arma.org/page/IGMaturityModel (last visited Aug. 14, 2018).

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, as 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 changing 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.

1. 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 business needs, information-related compliance requirements, and risk controls. Such a framework should categorize information types by content and context.[17] This will

---

[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 (Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2002)) by, *inter alia*, establishing internal controls for selecting and retaining service providers and 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 in their possession.

[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

normally require input from a wide range of subject matter experts, including, for example, business operations, HR, Accounting, Compliance, and Environmental.

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 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 functionally-segmented (or "siloed") structures governing data security, retention, and preservation, an organization could establish an Information Governance matrix. This matrix is a classification structure for the organization's information types similar to a traditional records retention schedule or data security grid but that integrates all established rules governing the organization's information types. It 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. The matrix should be designed to meet the needs of various audiences and multiple uses within the organization. It is essential, for all of the organization's business information, that the organization establish and clearly communicate specific roles and responsibility for complying with the integrated rules included in this governance matrix. Otherwise, "orphan data" can greatly increase the cost and risk of eDiscovery.

An organization should establish or adopt 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.

---

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.

[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 other business functions. Instances of the widget purchase order information may also, simultaneously, be associated with disaster recovery restoration, information protection issues (due to where versions of the purchase order are located physically or virtually), and applicable legal holds. The complexity of the digital environment, in which the same information content simultaneously exists in different locations and contexts and triggers different Information Governance rules, makes ontology a promising perspective for applying Information Governance to an organization's information.

2. Direction

Organizations should communicate to all information users (internal as well as external custodians, such as suppliers and contractors) the organization's requirements for Information Governance. Vehicles commonly used by organizations to provide such direction include policies, contracts, retention schedules, Information Governance matrices, procedures and protocols, and guidance and training (including certification and testing for comprehension).

The current state of Information Governance in many organizations involves an array of policies that directly or indirectly address Information Governance topics. Examples include a RIM policy, a communications policy, a computer use policy, an Internet and social media policy, a bring-your-own-device (BYOD) 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 a subset of Information Governance requirements 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 cohesive, actionable Information Governance policy. Similar to the Information Governance matrix, an Information Governance policy expresses in one place all of the organization's policy-level expectations for governance of information across the entire spectrum of possession, custody, and control, regardless of location, custodial, or organization boundaries. Then, specific sub-level policies can be established under the unified approval identified by the policy.

Further to this point, contracts with third parties are an important aspect of defining responsibility 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, and its standards of accountability for managing information resources, should be incorporated into such third-party contracts.[19] For example, engagement letters and billing guidelines with law firms should confirm the firm's obligations to protect and preserve information, confirm the organization's rights to conduct periodic compliance audits and review, and require the firm's 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 (including redundancy), protection, retention, preservation, and ultimate disposition. Organizations should also establish effective guidance and training regarding Information Governance, delivered in a way that confirms both awareness and

---

[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 ePHI created, received, maintained, or transmitted on behalf of the covered entity. 45 C.F.R. § 164.314(a) (2013).

understanding of policy rules, thereby empowering 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 in order to make information-related decisions consistent with the organization's Information Governance expectations.

3. 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 those from Legal, IT, Compliance, RIM, other administrative functions, and lines of business. People resources must recognize 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 methods and controls necessary for prudent 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 designed and implemented to address the program's scope and objectives. Information Governance technology resources should be procured only after requirements for such tools have been defined in a manner consistent with the organization's strategic objectives for Information Governance. Organizations should carefully match the capabilities of the contemplated technology against the program's desired objectives and document decisions regarding any gaps.

Although the full scope of technology implementation risks and requirements is beyond the focus of this document, organizations must recognize that implementation resources are also needed. These include project management tools and processes to be used as elements of the organization's Information Governance program.

4. 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

---

[20] Day v. LSI Corp., No. CIV 11–186–TUC–CKJ, 2012 WL 6674434 (D. Ariz. Dec. 20, 2012) (awarding sanctions against defendant for, among other things, defendant's failure to follow its own document retention policy).

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 for information users, their management, and those managing the Information Governance program.

Information Governance program objectives should be linked to observable and measurable outcomes. Compliance audits or comparable assessments of the program should be conducted on both a random and periodic basis, followed by appropriate corrective actions as needed. The program's measured outcomes should be periodically compared to target 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 and stakeholders to provide reasonable assurance that the program's objectives are being 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 an organization to dispose[23] of information that no longer provides value to the organization, if that information is not required for statutory or regulatory

---

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*, 3 (May 2013), https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.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 Federal Trade Commission's (FTC) 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 "[t]op management is responsible for setting an organization's direction and communicating priorities to employees and stakeholders." ISO 30300:2011, *supra* note 15.

23 In this commentary, the "disposal of information" concept 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.

compliance or legal hold purposes.[24] Despite this advice, many organizations struggle with making and executing on effective disposition decisions. That struggle is often caused by many factors, which include the following: (i) the incorrect belief that organizations will be forced to "defend" their disposition actions if they later become involved in litigation; (ii) the difficulty in appreciating how such disposition reduces costs and risks; and (iii) the difficulty in determining how to design and implement effective disposition as part of their overall Information Governance program. The Sedona Conference recognized the need for more scholarship on this topic. As a result, The Sedona Conference released a new publication in August 2018, *The Sedona Conference Principles and Commentary on Defensible Disposition*, to provide guidance to organizations, and the professionals who counsel those organizations, on developing and implementing an effective information disposition program.[25]

If there is no statutory, regulatory, or preservation obligation, information should be disposed of as soon as the likely business value of retaining the information is outweighed by the cost and risk 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,[26] 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.[27]

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 to minimize the risk of disclosure. Separately, organizations that operate in jurisdictions where individuals' privacy rights are protected by law may need to develop robust "mandatory destruction" capabilities. For example, the European Union's General Data Privacy Directive requires

---

[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] *See* The Sedona Conference, *Principles and Commentary on Defensible Disposition*, THE SEDONA CONFERENCE (Aug. 2018 Public Comment Version), *available at* https://thesedonaconference.org/publication/Commentary_on_Defensible_Disposition.

[26] 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 & Anthony Diana, *'Hoarders': The Corporate Data Edition,* LAW TECHNOLOGY NEWS (2012), https://www.law.com/legaltechnews/almID/1202581938140.

[27] ARMA Int'l, *Generally Accepted Recordkeeping Principles®*, Principle of Disposition, *supra* note 15 ("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.").

that the information relating to a person who seeks to be "forgotten" by a holder of his/her personal information must be demonstrably and promptly removed, on demand.[28]

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 of original documents versus copies of documents 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 various forms:

- A legal or litigation hold, i.e., the preservation of data for purposes of reasonably-anticipated or active litigation, regulatory inquiries, 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, which is an agreed-upon obligation that an organization has with its customers, vendors, divested entities, or other third parties that requires the preservation or disposition of information and exists separately from the organization's standard retention schedule[29]

1. 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 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.[30] 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.[31]

---

[28] GDPR, *supra* note 2.

[29] 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 as well as inconsistent obligations where different contracts prescribe different retention periods.

[30] 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.

[31] For more information, *see* ARMA Int'l, *Standards and Best Practices*, and *Generally Accepted Recordkeeping Principles*®, Principle of Disposition, *supra* note 15.

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, and other business-driven objectives) be considered as the organization formulates its retention protocols and schedule. 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 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.

2. Hold/Preservation Analysis

Before the organization disposes of any information, it should determine whether there are any legal, regulatory, or other obligations in place that require the organization to retain the information, regardless of its business value. To effectively identify its preservation obligations, it is advisable for the organization to develop and consistently implement protocols designed to track legal 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.[32] This exercise should be repeated whenever the organization decides to create, store, and use information from any new source, such as websites, social media, and portable devices.

It is important for the relevant constituencies within the organization—not just the Legal or Compliance Department—to understand that a legal hold supersedes all other RIM policies 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, the affected information can be placed back into the appropriate retention schedule.

3. 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 Conference Principles and Commentary on Defensible Disposition.*[33] In

---

[32] For further information on legal holds, *see* The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010).

[33] *See* The Sedona Conference, *Principles and Commentary on Defensible Disposition*, *supra* note 25.

addition, organizations considering disposition of inactive information sources should consult *The Sedona Conference Commentary on Inactive Information Sources.*[34]

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 data privacy, data protection, data security, records and information management (RIM), 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.[35] A common example involves the tension between data protection laws in the European Union that prohibit transferring "personal information" and United States federal court jurisprudence that mandates the production of such information during the discovery process.[36] In other circumstances, one jurisdiction may require an organization 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.[37] 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

---

34 *See* The Sedona Conference, *Commentary on Inactive Information Sources*, THE SEDONA CONFERENCE (July 2009 Public Comment Version), *available at* https://thesedonaconference.org/publication/Commentary_on_Inactive_Information_Sources.

35 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 case 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 that the comity factors outlined in *Société Nationale Industrielle Aérospatiale v. United States Dist. Ct.*, 482 U.S. 522 (1987), weighed in favor of disclosure.

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

37 For example, with respect to the transfer of information from France to the United States 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*, 482 U.S. at 546. 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.

organization should thoroughly document its efforts to reconcile the conflict and its resulting decision-making process.

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.[38]

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.*,[39] the court outlined factors to be considered in assessing the reasonableness of a record retention policy for a spoliation instruction, including the following: (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.[40]

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."[41]

---

38 *See* The Sedona Conference, *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, Principle 2 (Jan. 2017), *available at* https://thesedonaconference.org/publication/International_Litigation_Principles ("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), *available at* https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/feb-2012-dataprotection.authcheckdam.pdf ("[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.").

39 836 F.2d 1104 (8th Cir. 1988).

40 *Id.* at 1112.

41 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 an organization's intended retention period is 25 years and the media format it will be using has an expected life of 12 years, then specific planning will be required to 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 eDiscovery obligations.[42]

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.

1. Long-Term Digital Assets

The phrase "long-term" is used to mean a timeframe 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 especially 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 third-party services such as

---

[42] United States v. Universal Health Servs., Inc., No. 1:07cv000054, 2011 WL 3426046 (W.D. Va. Aug. 5, 2011).

cloud storage, software as a service (SaaS), etc.), the contractual agreements between the customer and provider.[43]

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 oversee 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 eDiscovery 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 have not been accessed recently.

In addition to reliance on end-users, 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 the following: (i) optimizing the governance of information for traditional RIM; (ii) providing more efficient and more efficacious means of accessing information for eDiscovery, compliance, and open records laws; and (iii) advancing sophisticated business intelligence across the organization.

1. 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."[44] 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," "computer-assisted review," and "technology-assisted review" are terms used in the

---

43 For a more detailed explanation of the specific areas of risk for digital assets, *see* Appendix C.

44 Arthur L. Samuel, *Studies in Machine Learning Using the Game of Checkers*, IBM JOURNAL OF RESEARCH & DEV. 3(3):211-229 (1959).

eDiscovery arena to describe the process whereby humans code sets of data into responsive and nonresponsive categories until the software can reliably analyze the remaining huge repositories of data.[45] 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.

2. 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 RIM 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.[46] Organizations increasingly utilize predictive analytics to assist in categorization functions, where individuals train software to differentiate between types of records.

The first judicial opinions approving the use of predictive coding and technology-assisted review techniques for document review in eDiscovery were published in 2012.[47] In one case, the court stated that "the Bar should take away from this 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."[48] An important study by the Rand Corporation, anticipating this new direction in the law, concluded that predictive coding may significantly reduce eDiscovery costs by reducing the number of documents requiring eyes-on review.[49] The use of technology-assisted review for the exploration and classification of large document collections in civil litigation has evolved from a theoretical possibility to a valuable tool in the litigator's toolbox.[50]

---

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

46 The National Archives and Records Administration (NARA) 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), *available at* http://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

47 *See, e.g.*, Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182 (S.D.N.Y.), *approved and adopted*, 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., 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).

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

49 Nicholas M. Pace & Laura Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery,* RAND CORPORATION (2012), *available at* http://www.rand.org/pubs/monographs/MG1208.html.

50 *See* The Sedona Conference, *TAR Case Law Primer,* 18 SEDONA CONF. J. 1, 3 (2017).

3. Predictive Analytics and Compliance

Predictive analytics is also increasingly being utilized by organizations outside of the eDiscovery context, including in investigations and as an element of compliance programs. Predictive analytics is being used as an early warning system in compliance programs to predict and prevent wrongful or negligent conduct that might result in data breach or loss. 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.

4. 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. Organizations are beginning to use predictive analytics to develop business intelligence about the organization itself, 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. 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[51] and, regardless, is prudent given the inevitability of organizational and environmental change. Organizations, therefore, should periodically review and update their Information Governance program.

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,

---

[51] 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 ePHI. 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 GLBA 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).

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 do the following:

- Identify any significant changes in its lifecycle practices for information
- Identify significant changes in applicable compliance requirements and risks regarding its information
- Review the organization's strategic objectives for Information Governance considering internal or external changes
- 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.

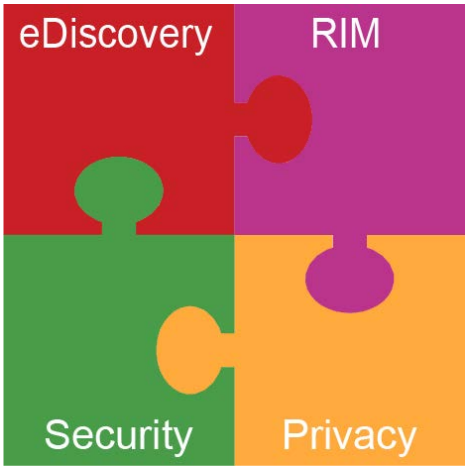
No bright-line rule governs how frequently an Information Governance program should be reviewed. As with other business-driven initiatives, the frequency of review will most likely depend on many factors relating to the organization.[52] If an organization is rapidly changing through frequent acquisitions 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 record-keeping, data security, and operational requirements. Further, an organization may be impacted by external pressures, such as regulations subject to frequent modification or regular compliance audits

[52] 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 (1984), *overruled on other grounds*, Brehm v. Eisner, 746 A.2d 244 (Del. 2000).

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 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.

As a result 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 the organization's strategic objectives for information.

APPENDIX A: INTERSECTIONS



Intersections Create Opportunities and Challenges

Although the functional areas of Records and Information Management (RIM), eDiscovery, Privacy, and Security are frequently separate, a successful Information Governance program requires them to work together. As there is some natural overlap among the four groups, this provides opportunities to combine resources and budgets. Conversely, the goals of the 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	eDiscovery Intersection with Functional Area	Privacy Intersection with Functional Area	Security Intersection with Functional Area
RIM ***Primary Focus:*** *Ensuring that records and information are properly maintained, accessed, and ultimately disposed of in accordance with statutory and regulatory requirements and with consumer expectations*	**N/A**	**Potential Synergy:** ● Share 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 ● Enable an organization to know what it has and identify, preserve, retrieve, search, produce, and appropriately destroy data in normal course of business ● RIM protects against loss of content that could lead to sanctions, financial loss, and brand risk during eDiscovery ● RIM serves as evidence of official policy and helps ensure that evidence can be authenticated **Potential Friction:** ● RIM could retain drafts or outdated content due to relevancy ● RIM focus could be more narrowly targeted to "records," while eDiscovery focus is ESI	**Potential Synergy:** ● Define requirements for identification and classification of sensitive information **Potential Friction:** ● RIM may need wide access and distribution, while Privacy seeks limits	**Potential Synergy:** ● Ensure that sensitive information is properly identified, 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	eDiscovery Intersection with Functional Area	Privacy Intersection with Functional Area	Security Intersection with Functional Area
eDiscovery ***Primary Focus:*** *Preserving and processing electronically stored information that is potentially relevant to impending or ongoing litigation in a timely, auditable, and efficient manner*	**See RIM/eDiscovery intersection above**	**N/A**	**Potential Synergy:** ● Identify at point of creation information subject to privacy regulations to reduce risk that private information will be produced **Potential Friction:** ● Producing private information protected by another country's laws can result in civil or criminal sanctions ● Refusing to produce private information may result in civil or criminal penalties under U.S. laws	**Potential Synergy:** ● Ensure that sensitive data and information are available, if relevant, and that out-of-date information is disposed of according to legal and regulatory requirements ● Satisfy an organization's "duty to preserve" for forensic collections **Potential Friction:** ● Security encryption requirements can hamper eDiscovery efforts
Security ***Primary Focus:*** *Ensuring the confidentiality, integrity, and availability of information and assets*	**See RIM/Security intersection above**	**See eDiscovery/Security intersection above**	**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 Chief Executive Officer (CEO) or Chief Operating Officer (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.

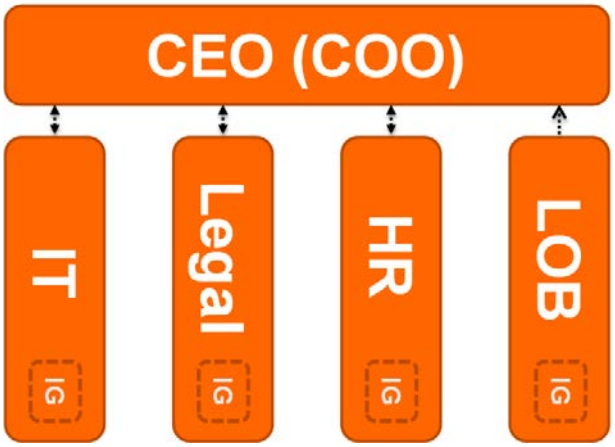
Maturity and Independence

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 deciding 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, Security, eDiscovery, etc., are intentionally not shown because they generally reside within a stakeholder department.

Immature

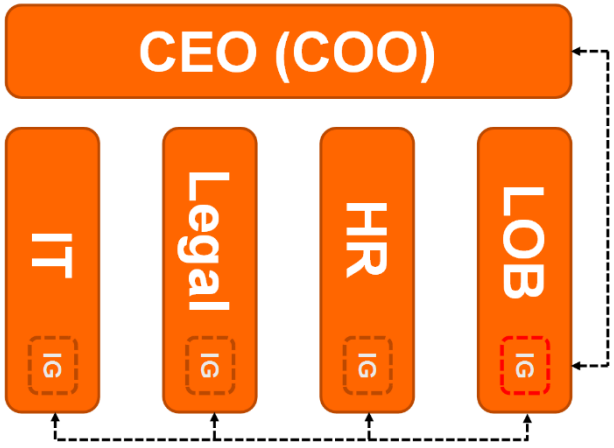
Immaturity is characterized by a lack of over-arching coordination of Information Governance stakeholders and no single point of accountability to the CEO or COO for overall governance of information**.**



At the immature end of the maturity continuum, lack of coordination creates a potential for missing important requirements. 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 that 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

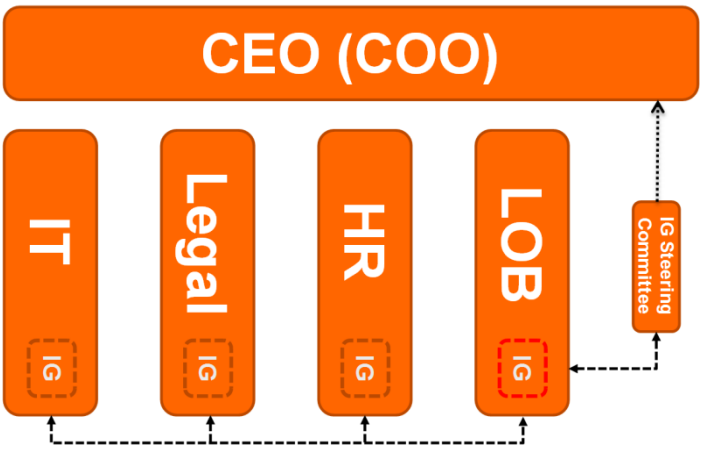
At this area of the maturity continuum, ownership of Information Governance process resides within a stakeholder department.



This creates a potential conflict of interest, due to misaligned incentives.

More Mature

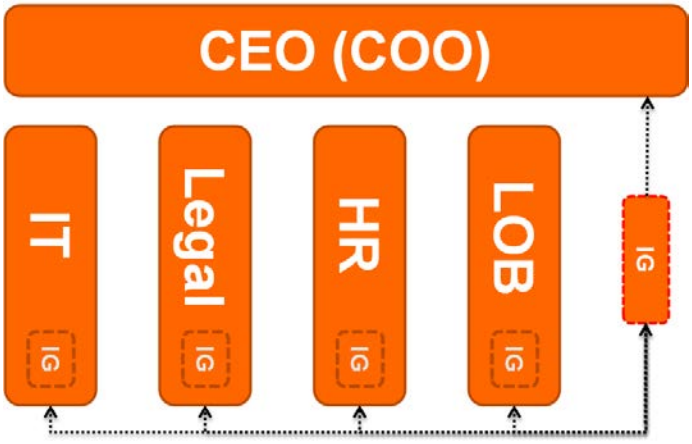
At this area of the maturity continuum, ownership of Information Governance process resides in a stakeholder department but is accountable to a steering committee of C-level executives from the stakeholder departments who are accountable to the CEO or COO.



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 Information Governance function is characterized by an executive who resides in a separate Information Governance department and 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 the following:

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 a guarantee that the file has not 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 (i) the level of integrity required both for the digital asset in question and the technologies required to read and access the data and (ii) the level of difficulty involved in repairing or recovering damaged digital information.

Careful consideration should also be given to the file format, storage medium (including the configuration of that storage medium), and the circumstances of operation and storage 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 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 the following:

- being able to access information in a timely manner (for example, within applicable service-level agreements, contractual requirements, or timeframes indicated by legal requirements); and

- being available within an agreed-upon lead time (depending on business need).

Note that availability can apply to 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) and 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 the following.

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—especially those held for reference purposes—but not for binary files, such as audio files or Computer Aided Design (CAD) files. Micrographics may also not work well for files that need to be in digital format 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. For example, regulated utilities or pipelines often involve document retention periods of decades, which can be 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 its originally form. 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 media, 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 return on investment (ROI) for particular projects.

A typical ROI analysis weighs the benefits of a 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.[53]

The quantifiable benefits from pursuing Information Governance generally fall into four main categories: optimizing organization value, risk reduction, hard cost avoidance, and soft cost avoidance.

Optimizing Organization 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 benefits of an Information Governance program, which add to organization value, and we provide some examples:

- **Effectiveness** (e.g., document-centric collaboration tools)
- **Cost/efficiency** (e.g., imaging/workflow solutions replace traditional paper-oriented processes)
- **Customer service** (e.g., customer-relationship solutions that lead to better market penetration and customer satisfaction)
- **Competitive advantage** (e.g., more modern tools and reliable information allow speedier delivery of goods or services to customers)
- **Revenue** (e.g., as a result of enhanced social media and web presences and solutions)[54]

---

53 *See generally* SUNIL SOARES, SELLING INFORMATION GOVERNANCE TO THE BUSINESS: BEST PRACTICES BY INDUSTRY AND JOB FUNCTION (MC Press 2011) (providing insight into the best ways to encourage businesses to implement an Information Governance program).

54 *See First 100 Days: Enterprise Content Management Initiatives*, GARTNER (July 7, 2011), *available at* http://www.gartner.com/id=1739415.

A core benefit of an Information Governance program is to ensure that information used for different purposes across the organization—e.g., for sales and marketing, but also for planning, billing, fulfillment, financial, customer feedback, and other downstream purposes—is reliable or trustworthy, accurate, and in formats usable across platforms or applications. Achieving these objectives requires that the IT department understands 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).[55] 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.[56] 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.[57]

Mergers and acquisitions, or technology upgrades, also present opportunities (and challenges) for improving data quality and organization revenues by, for example, merging (and purging) customer lists to identify strong customers across multiple business lines.[58]

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 electronically stored information (ESI) is often stored away, rarely accessed, and often never reassessed 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 eDiscovery, while providing little or no benefit for other organizational areas, such as business units. Through proper Information Governance, organizations can recognize

---

55 *See, e.g.,* Soares, *supra* note 53*,* at 149.

56 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 BIG DATA & ANALYTICS HUB (July 5, 2013), *available at* http://www.ibmbigdatahub.com/blog/business-and-it-collaboration-essential-big-data-information-governance.

57 *See, e.g.,* The Sedona Conference, *Commentary on Finding the Hidden ROI in Information Assets*, 13 SEDONA CONF. J. 267 (2012).

58 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* note 53, at 69.

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:

- **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.

- **Privacy Breaches:** A myriad of regulations applicable to particular sectors in the United States (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.

- **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.

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

- **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 program 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 program, often arise from the following areas:

- **Storage:** Storage and maintenance costs can be radically reduced by rationalizing data storage options, eliminating outdated information assets 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 and associated backup overhead and better enable data disposition in line with organizational policy.

- **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.

- **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.

- **eDiscovery 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.[59]

Soft Cost Avoidance

Improved Information Governance also saves 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:

- **Economies of Scale:** Managing information on an ad hoc basis can result in overlooked requirements and risks, unrealized benefits, 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 information assets are handled.

- **Organizational Inefficiencies:** Organizations with excessive amounts of uncategorized information assets 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 repurposing of institutional knowledge, and enhances continuous improvement efforts.

---

[59] A widely-cited 2012 Rand survey states that the review process alone averages $18,000 a gigabyte, meaning that with collection, preservation, hosting, etc., eDiscovery costs can easily exceed $20,000 a gigabyte. Nicholas M. Pace & Laura Zakaras *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*. RAND CORPORATION (2012), *available at* http://www.rand.org/pubs/monographs/MG1208.html.