Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

InfoPAK[SM]

Information Governance Primer for In-house Counsel

Sponsored by:

Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA

Information Governance Primer for In-house Counsel

September 2016

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

Corporations face a number of legal, regulatory, privacy, and other challenges managing files, emails, and other types of electronic information as well as paper documents. Traditional siloed approaches of having separate records, discovery, privacy, or other programs often are ineffective. Increasingly, organizations are developing and launching comprehensive Information Governance (IG) programs that reduce risk, ensure compliance, lower costs, and perhaps most important, increase employee productivity. Working in collaboration with other groups, in-house counsel serve as key stakeholders in these initiatives.

This InfoPAK is a primer for in-house counsel starting, building, executing, and refining an Information Governance program. It explains why companies are launching these programs, how to develop an IG committee, key steps increating a business case and how to develop a program roadmap. It also addresses specific Information Governance areas, such as updating a record retention schedule, creating a data security policy, developing a proactive ligitation readiness program, as well as objectively measuring the effectiveness of these areas. This InfoPAK provides practical advice and intends to educate and empower in-house counsel to drive these cross-functional initiatives within their organization.
This information should not be construed as legal advice from Contoural, or legal advice or legal opinion on specific facts, or representative of the views of ACC or any of its lawyers, unless so stated. This is not intended as a definitive statement on the subject but a tool, providing practical information for the reader. Readers should consult with competent legal counsel for professional assurance that this InfoPAK's information, and any legal interpretation of it, is appropriate to each reader's particular situation

This material was developed by Contoural, Inc.. Contoural, Inc. is the 2016 co-sponsor of the Information Governance Committee. For more information about author, visit their website at www.contoural.com or see the "About the Company" section of this document. ACC and Contoural wishes to thank members of the Information Governance Committee for their support in the development of this InfoPAK.

Contents

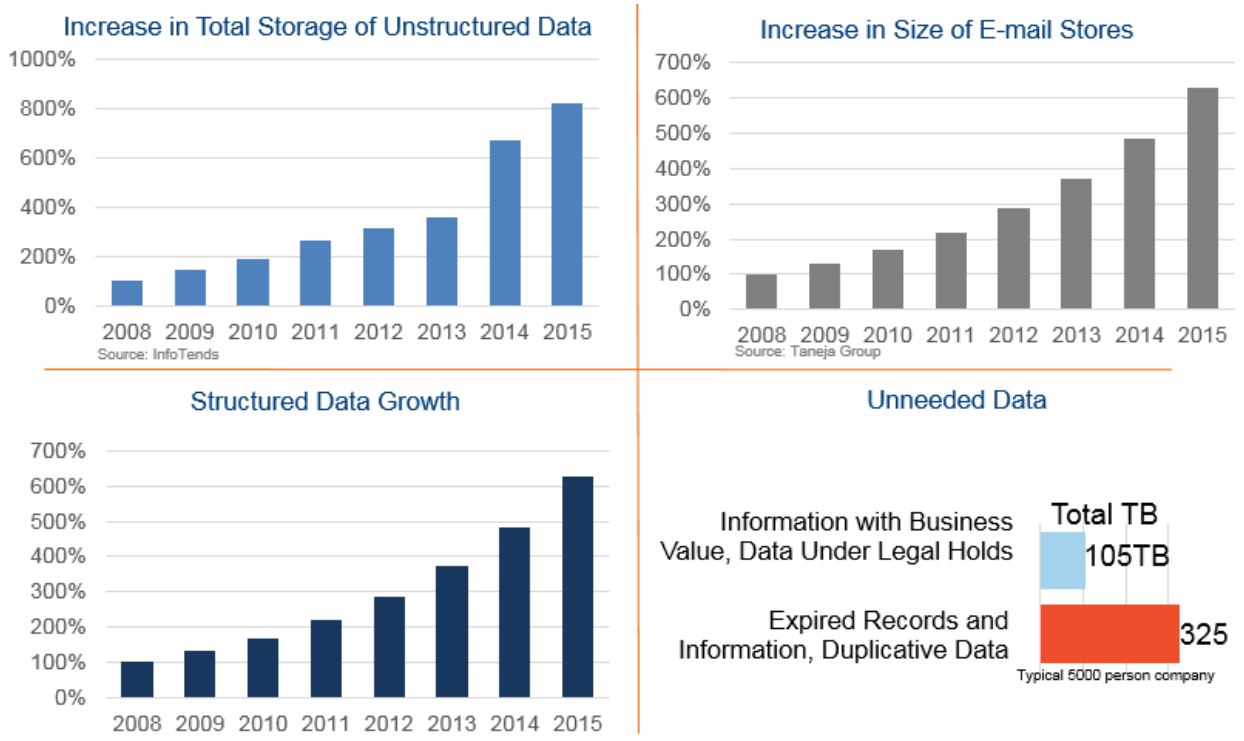
I. Why Information Governance?

Faced with increasing data volumes, more stringent legal and regulatory recordkeeping requirements, stricter privacy rules, increasing threat of breaches, and decreasing employee productivity, corporations are reorganizing separate record management, discovery, security and IT programs into comprehensive Information Governance (IG) programs addressing both paper and especially electronic information.

A. The Problems of Managing Documents and Data

1. Ongoing Accumulation of Paper and Electronic Information

Companies have seen a significant increase in the volume of both paper and, especially, electronic documents and data created and received. Today, the average employee sends and receives more than 100 emails per day, and 25 percent of these contain attachments.[1] While many organizations still have large stores of paper documents, increasingly, business is being conducted through electronic media. According to a recent study from the University of California, Berkeley, more than 96 percent of all information in an enterprise is in digital format, and even 70 percent of all paper documents are copies of electronic documents. The average employee also creates or modifies 20 or more files per day. And now, with the advent of social media (e.g., Facebook and Yammer), as well as connected devices communicating through Internet of Things (IoT) systems, the resultant surge of data creation is creating new compliance challenges for many organizations.



While paper use in North American offices peaked in 1998 in most organizations, the retention of electronic information is accelerating. Data volumes are doubling everything three years. This data includes emails and files that contain records, privacy information, intellectual property, and other high value business information. On the other hand, a large percentage of this digital "pile" is considered ROT (*R*edundant, *O*bsolete and *T*rivial) information. On average, more than 65 percent of an organizaton's unstructured data is composed of files across file shares, desktops, and other repositories, are expired records, records with little or no business value, or are convenience copies of documents managed elsewhere. Both too many documents and too much data are causing problems.

a. New Landscape Creates New Risks

Not only are organizations accumulating more electronic information, the legal, regulatory, and security landscapes are becoming more challenging. These challenges and risks have impacts across the organization:

- *Increased Legal and Regulatory Recordkeeping Requirements* – The average U.S. Corporation faces more than 30,000 legal and regulatory recordkeeping requirements. These include federal, state, and industry-specific requirements. Newer regulations, such as Dodd Frank, as well as updates to existing retention requirements from the Environmental Protection Agency, for example, expand the requirements for recordkeeping and require that information be more accessible. Organizations with a global footprint facing regulations from multiple countries face another layer of complexity.
- *Discovery Risks and Costs* – The ongoing accumulation of both paper and electronic information creates very acute challenges when organizations face discovery in litigation. First, the sheer volume and expanse of electronic information increases the risks of being non-responsive to a discovery request. Not knowing what a company has often forces them to look through everything. Second, the increasing volume and lack of controls significantly increases discovery costs and impacts litigation strategies. Additionally, new discovery rules in the U.S. and Canada can benefit those organizations that effectively manage their information, as well as penalize those that do not.
- *Increased Regulatory Inquiry and Shorter Timeframe to Produce Information* – The past eight years have seen an increase in both industry-specific regulatory sweeps as well as increased enforcement of existing regulations, such as Federal Corrupt Practices Act and U.K. anti-bribery laws. During an inquiry, regulators not only seek official records, but also any other documents or data that may be relevant to their investigation. Moreover, regulators want them quickly, often seeking these documents within days.
- *New Stricter Privacy and Data Protection Requirements* – Across the globe, governments are enacting stricter and more punitive privacy and data protection requirements. Led by Europe, these requirements mandate that information

about citizens be secured, used in appropriate ways, and can be deleted upon request. This type of information lives not only in databases, but also in files and emails.

- *Risks of Data Breaches* – Criminal groups (often based overseas) as well as activist disclosure organizations, such as Wikileaks, are targeting and breaching electronic data stores of many organizations. Increasingly, these breaches are not only attacking traditional targets, such as financial systems, but also employee email communications, files, and other lightly managed and secured information. Organizations facing breaches not only face significant fines and expensive remediation processes, but also may suffer significant reputational loss.
- *Intellectual Property* – Organizations continue to face challenges around asserting their ownership of intellectual property (IP) against competitors, well-funded "patent trolls," and other litigants. Establishing ownership is often based in "organically" grown emails, files or other documents spread across the enterprise. Management and control of these documents are key to an effective IP strategy.
- *Mergers, Acquisitions, and Divestitures* – Successful and timely mergers, acquisitions, or divestitures often depend on the ability of organizations to identify, classify, and either integrate or separate large quantities of information throughout the organization.
- *Record and Data Storage Costs* – Over-retention of both paper and electronic information continues to drive both paper record storage and electronic data storage costs, often diverting resources from higher value projects.

b. Employees "Drowning" in Their Own Information

While poorly managed information creates a number of legal, regulatory, and security challenges, it can also significantly impact and decrease employee productivity. Employees who have adopted a "save everything" approach for email and files (documents) soon find it difficult to find their own information among the clutter. Gartner Group estimates that the average employee wastes more than 3.5 hours per week locating emails or the correct version of files.

This problem is compounded when departments face employee turnover. Today, many employees store key information in their own individual silos on file shares or within their own personal email stores. When there is employee turnover, this information is effectively lost and the employee's successor is often forced to reinvent the wheel. Legal, IT, and other key stakeholders often wrongly assume that employees are happy with current "save everything everywhere" when, in reality, there is significant latent pain both by employees and within the business units.

"I spent my first three months on the job searching through my predecessor's email. I had to look for everything from offer letters to employee reviews, spending hours every week. What a nightmare." – Vice President of Human Resources for a Mid-sized High Technology Company

B. Where Traditional, Siloed Programs Fall Short

Responsibility for managing documents and data may fall across legal, records management, compliance, privacy, IT, information security, audit, HR, and individual business units. Traditional programs, however, where responsibility is "siloed", fall short. It is a problem that many groups share and yet no one group really owns:

- *Records Management* - May be responsible for official records, but not management and control of the non-record documents.
- *Legal* - May be responsible for policy creation but depend on other groups to execute these policies.
- *IT* - Manage data storage, but not the actual content (which is owned by the business units).
- *Litigation* - often is focused on matter-specific litigation but with no charge to proactively address management of documents and data outside of litigation.
- *Information Security* - Is responsible for securing the firewall, but has little say on what privacy data is stored where.
- *Privacy* - worries about privacy data in both records and non-records, but is limited in its ability to drive disposition.
- *Business Units* - Often do not care about any of this and want to be left alone to run the business, except they cannot even find their own important information in the clutter.

What's more, mulitple groups may independently undertake similar tasks, such as data mapping. Also, the needs of employees and business units are often ignored. It is common to find disjointed initiatives and the lack of coordination among groups which is both ineffective and wasteful.

Everyone wants better control of information and data because doing so provides cost saving, productivity, innovation, and compliance benefits, but (naturally) no one wants to end up owning the whole problem. The result is that organizations get stuck, and the problems just get worse.

Increasingly, organizations are taking a unified information governance approach to controlling their documents and data. Instead of having multiple different initiatives at a departmental or divisional level, an organization-wide IG program strives to create work streams that address common needs and, at the same time, minimize risk. It seeks coordinated control of data and documents for retention, business use, access, and disposition. Information governance recognizes that the key is gaining effective control of data and documents foremost, and that good control through a single program can serve multiple records, discovery, privacy, and productivity matters.

To better address the shift over the last decade from paper to electronic media, in addition to taking a more comprehensive approach, organizations are moving away from a paper-centric paradigm and taking a more electronic media-capable approach.

Traditional Paper-centric Approach	Electronic Media-capable Approach
Media-specific approach that addresses mainly paper	Content-specific approach capabley of addressing paper and especially electronic content
Detailed Records Retention Schedules with hundreds of categories	Compliant yet "Bigger Bucket" retention categories for easier classification
Manually oriented record classification strategies	Easier, faster, intuitive, and sometimes automated classification procedures
Documents classified for retention periods	Documents classified for a broader information governance framework including retention, data security, access controls, and collaboration
Many records printed out on paper as the official copy	Most documents managed in electronic format
Information stored in difficult to access locations, such as offsite storage	Employees and departments have easy access to their documents and data

Employees self-verify compliance	Regular system audits ensure policy defensibility

A key element of most IG initiatives is that they combine legal and regulatory requirements with employee behaviors and business needs, with a very strong focus towards measurable execution. No two IG programs will necessarily look the same from organization to organization as they must reflect the differing business realities that organizations face.

C. Information Governance Defined

Formally speaking, information governance is the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving, and disposition (usually deletion) of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.[2] More simply stated, information governance combines traditional records and information management (RIM), eDiscovery, privacy, security, defensible disposition, and employee productivity into real-world, executable strategies that allow organizations to better manage, retain, secure, make accessible, and dispose of their information and data through cross-functional initatives.

Information Governance programs need to be both comprehensive in their approach and tactical in their execution. Taking a big picture view can allow single initiatives to accomplish a number of business goals. Successful IG programs are developed with this larger view in mind. At the same time, it is important that these initiatives be broken into discrete tasks, and that the benefits can be both measured and easily understood. While formal definitions may be technically accurate, often it is more useful to describe these programs in plain, simple terms.

D. Case Studies: IG Programs and Their Impact

One of the best ways to understand Information Governance is to review the impact that IG programs have on organizations. The following are three samples of IG initiatives and their impact:

Sample IG Initiatives and Their Impact
Health Insurance Organization Classifies and Deletes Email ***Information Problem:*** A health insurance provider needed to get better control of emails.

For many years, employees had adopted a de facto "save everything" policy saving their emails in their own personal folders. These emails contained a variety of active records, privacy information, corporate confidential data as well as significant amounts of low business value or expired information. In addition to the security risks of these lightly managed emails, the ongoing accumulation of this data significantly increased discovery costs and was burdensome during regulatory inquiries.

IG Projects: The company embarked on an email policy and archiving project. This included email policy updates, technology acquisition, employee training, behavior change management, and audit programs.

Impact: Emails that were records or had sensitive information were properly classified and more than 45 million emails were defensibly deleted during the pilot – all with no employee complaints.

Global Manufacturer Manages and Protects Intellectual Property

Information Problem: A global manufacturer was concerned about securing and managing its intellectual property. Much of its IP resided in files and other documents stored on file shares and employee desktop systems in its offices throughout the world. In light of data breaches perpetrated by overseas entities, the board of directors' audit committee raised concerns about managing and securing this information.

IG Projects: The company first updated its data security classification policy, making it both simpler and more comprehensive. Next, it implemented a data placement strategy (DPS), defining appropriate repositories for all types of information including appropriate security controls. Once these were in place it stored and secured both new documents as well as older information into these systems.

Impact: Previously, only 15 percent of the company's IP was managed in accordance with the data security classification policy. After this initiative, subsequent audits revealed that this had flipped and 85 percent of the information was being managed appropriately. Over time, the company continues to address the remaining 15 percent.

Life Sciences Company Drives Employee Innovation Through Better Records Management

Information Problem: Through a series of acquisitions, the retention and disposition processes for a mid-sized life sciences company had become disjointed. While this raised compliance concerns within the legal department, senior management was more concerned with increasing employee innovation and collaboration, especially across the

newly acquired business units.

IG Projects: In an innovative move, the legal department partnered with IT and rechristened their records program into an employee innovation program. They conducted an information types inventory, updated their record policies, and mapped what data lived where. They used this information when they moved to a new document management system.

Impact: They were able to identify significant amounts of duplicate information, as well as content that needed to be made more accessible across the organization. Users were encouraged to better collaborate, and controls were put in place to better manage and expire key content.

The above three examples illustrate IG gains across three separate industries. These examples demonstrate that Information Governance is not limited to just a few industries. Rather, all sizes of organizations – from 100 person organizations to those with more than 250,000 employees – and all types of organizations – both public and privately held – across all industries see the need and are launching IG programs.

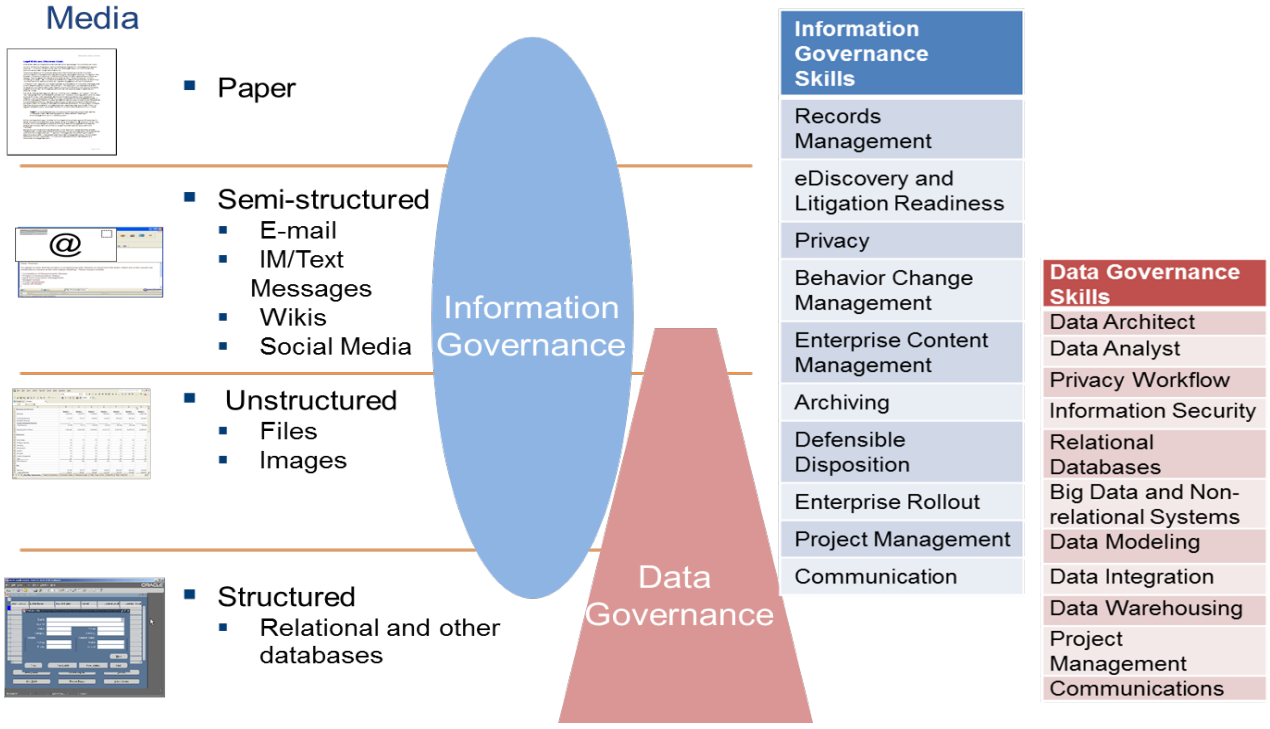
E. The Difference Between Information Governance and Data Governance

What's the difference between Information Governance and Data Governance or are they the same thing? How should each be managed? This is an area of significant confusion that often comes up when an organization is considering launching an IG initiative. Information Governance and Data Governance are different yet complementary activities. Understanding the differences and intersection is key to keeping both on track.

Information Governance addresses records and information management, litigation readiness, control of private and other sensitive information, and employee productivity. Information Governance primarily addresses paper, semi-structured media, such as email and unstructured media, including files and sometimes databases in structured applications. As discussed in this InfoPAK, IG also addresses data placement, employee training, and behavior change management as well as defensible data disposition. The types of technologies to support IG programs include enterprise content management (ECM), archiving, discovery, and other technologies for managing content. It is about becoming compliant, reducing costs and risks, and enabling employees to be more productive.

Data Governance is the processes and policies to ensure that data is managed as a single point reference. It is about leveraging large amounts of data to answer big questions, such as who to sell to, how to price products, and what new markets should be approached. It encompasses areas such as master data management, data quality, and data modelling and often uses newer types of technology, such as Hadoop, that can pull together different data sources.

For example, a bank that provides a customer's checking account may want to cross-sell mortgage refinancing. This may involve bridging the systems for managing accounts with a marketing database for mortgages. Data Governance programs often pool a number of structured media, such as databases and sometimes unstructured file data, into large "pools" against which queries can be run. Data Governance has long been associated with structured data living in a type of database (called a relational database), but can also incorporate individual files or even emails. These types of projects are sometimes called "big data" projects and serve to drive revenue or increase profits.



While both of these initiatives strive to manage data better, the tasks, outputs, and skills required for each are fairly different. Without a clear understanding of how these areas are different, it is easy for IG activities, such as creating more efficient discovery processes, to

"get lost" in a larger data governance agenda. Note that a strong Information Governance program can complement and assist a data governance initiative. For example, ensuring that emails and files to be ingested into a data governance "data lake" do not contain privacy or other sensitive information can keep the data lake "unpolluted" and compliant. When contrasting these programs, focus on project tasks and outputs and avoid esoteric technical definitions, as this will help clear up potential confusion.

II. Developing Your IG Team

A proper IG program addresses seemingly overwhelming volumes of information, often sensitive and fraught with risk. While the pain of poorly managed information can be particularly acute for in-house counsel, the temptation to execute these initiatives alone should be avoided. The most effective programs are composed of legal, IT, risk, compliance, security, privacy, records management and business experts. No one person or group has the expertise to address all of the functional aspects of an IG program, and collectively, a well-established team will be better positioned to get the job done.

A. Why In-house Counsel Should Be Involved in Information Governance

When faced with Information Governance challenges, often the first question asked by in-house counsel is: Why me? In-house counsel ask if and when they should be involved, and wonder if it is better to let this be, for example, entirely an IT initiative, especially as a big focus is on the remediation and proper management of electronic data. At a time when many legal department budgets are being scrutinized, it is fair to ask if in-house counsel needs to be the one to lead this dance. In a word, yes. Legal should participate in IG programs for the following reasons:

- *Legal Experiences the Pain of Poor Information Management* – Not knowing what information resides where forces organizations to directly drive up eDiscovery risks and costs and create overly broad legal holds. Significant amounts of ROT (Redundant, Obsolete and Trivial) data drive up document review times and costs. Failure to retain and provide accessible records can make dealing with regulators more difficult. Privacy and other sensitive information stored in the wrong place can greatly increase the likelihood of a data breach. Legal, perhaps more than any other group, bears the consequences.
- *Legal Owns Many Policy Components* – In most organizations, records retention and destruction, privacy, legal hold, and other key information management policies are the purview of legal. It is critical that these policies be designed to be both compliant and executable. These policies should be created or updated early in the process.
- *Legal Helps Avoid Risk* – Part of legal's charter is to proactively identify and avoid risks to the organization. Perhaps more than any other group they must be forward-thinking, anticipating changes in the legal, regulatory, and business environment, and preparing the company to deal with these changes.
- *Legal Often Has a Respected Voice to Senior Management* – Legal exerts a tremendous influence, unlike other groups, within an organization. Both senior management and boards legal's voice.

- *IG Has an Opportunity for Legal to Add Value* – Organizations often start executing IG programs to address legal or compliance issues, and find that these programs also drive employee productivity and save money. The nature of these programs often changes from something an organization needs to do to something it wants to do. Spearheading these programs is a way for in-house legal departments to demonstrate value.

B. Who Should Own (and Pay for) Information Governance?

While clearly in-house counsel should be involved in Information Governance, should they own the entire program? And by the way, who pays?

Program ownership varies significantly across different organizations.

1. Approach 1: Single Department Ownership

Sometimes a single department, such as legal or IT, has ownership for most parts of an IG program. This structure is often a legacy of when records management reported into legal and was primarily responsible for managing paper. That structure is now changing. Records management responsibilities are expanding to include electronic documents and privacy, for example, yet the group continues to report directly into the same function (i.e., usually legal).

The advantage of single department ownership is that roles and funding are clear. Furthermore, the institutional knowledge of past practices is retained within the same group. For example, the facilities group, having always managed paper, knows where the paper repositories live. The clear disadvantage of this approach is that both the skills and capabilities for executing these programs lie across multiple groups. The facilities group is not likely to be an expert in the archival of electronic information and, therefore, is likely to promote the continued printing and retention of hardcopy documents.

This model is becoming less common. As organizations understand the requirements of these initiatives, ownership is often transitioned to multiple stakeholders. Organizations wanting to embrace this type of model need to ask themselves if it will really work for them.

2. Approach 2: "Chief Information Governance Officer" Responsible for Multiple Functions

During the past few years, there has been much discussion about the creation of a Chief Information Governance Officer (CIGO) position. A CIGO, as the name infers, has direct

responsibility for many (if not most) components of an IG program, including policies, processes, technology selection, training for records management, privacy, eDiscovery, disposition, and other components. The idea behind the CIGO is that a single individual providing an integrated approach serves the management of information, documents, and data best.

The advantage of this approach is that it drives a type of economy of scale, combining multiple drivers into single projects. The biggest drawback to this approach is that many departments are unwilling to cede control, ownership, and budget to another function, and senior management does not understand the nature of these issues well enough to empower this type of position. Over the long term, organizations will be creating many more CIGOs. Today, this position remains relatively rare.

3. Approach 3: Cross-Functional Steering Committee Ownership

By far, the most common approach when launching an IG initiative is to create a cross-functional committee composed of multiple stakeholders. Typical committee members include legal, IT, compliance, privacy, audit, risk, and sometimes HR and business units. Each stakeholder is still responsible for their area of expertise (legal still creates policies, for example) but these activities are done through an integrated and coordinated plan.

4. The "Elephant in the Room" – Who Should Pay?

Which department is going to pay? IT thinks Legal should pay because Legal will benefit from the archiving solution. Legal thinks IT should pay because technology is involved. Or is it the business units who should pay? One of the risks in engaging a number of stakeholders in this discussion (and understanding their needs), is that it also creates conflicting expectations about who should pay. There have been situations where an e-mail archiving system, for example, would have saved a company literally millions of dollars, but the project was stalled due to arguments over who would pay. The greatest risk is that no one initiates these discussions for fear that speaking up first will somehow tag them as project funders.

Experience has shown that it is best to get these issues out on the table early. Clearly, IG initiatives do cost money, but they also can save even more money. Often when the committee highlights the risks of not having a program, senior management will fund or start funding these programs through other sources. Some organizations have been successful in attaching these initiatives to risks that the board of directors' audit committee highlighted. Sometimes these committees negotiate that legal will pay for the policy and IT will pay for the technology components. When unspoken, what appears to be a budgetary no-go, a number of creative funding solutions come to light when discussed.

C. Engaging Key Stakeholders

1. Developing an Information Governance Steering Committee

An effective IG initiative can be a big win for an organization, and getting started can be tricky, as many of these types of initiatives veer off the road and get stuck in the mud. How it is approached and with whom – decisions made early in the process – often dictate the success or failure of a program. While every organ ization is different, successful programs share some common approaches.

One of the biggest challenges in starting an IG progam is getting separate functions, that have separate budgets, to work together on an integrated initiative. To overcome these challenges, in-house counsel, working with IT and others, should consider forming an information governance steering committee.

Steering committee members can include:

- *Legal* – Records Management, Litigation.
- *Compliance* – Privacy, Audit, Risk Management.
- *IT* – Messaging, Infrastruture, Information Security.
- *Business Units* – For example, HR, Engineering, and Finance, with the final composition varying from organization to organization.

While the temptation may be to develop the strategy alone (or with a small group) and then engage other groups later in the process, it is better to start with a larger group. Although a larger group may seem unwieldy, it is better to be more inclusive earlier in the process than having an excluded group stall the initiative later on in the process.

Early on, round-table discussions should be conducted to identify issues and generate stakeholder buy-in. A suitable senior management sponsor (or sponsors) to whom the committee is accountable should also be identified. A "charter" that outlines the specific business issues to be faced, responsibilities of team members, and expected business benefits of the IG program should be developed.

Teaching others about the benefits of records management can seem quixotic, but there are approaches that work. Rather than trying to communicate the entirety of information governance, focus on the benefits it provides to each stakeholder. Consider stakeholder and other employee pain points and the risks inherent in their daily work, and propose individual benefits provided by better management of records.

2. IG Committee Authority

An effective IG committee strikes a balance of including committee members to decide on large and cross-functional issues while still allowing individual business units the latitude to execute their individual projects or pieces.

Some areas of committee authority include:

- *Policy Decisions* – Committees often review important policy decisions including retention, data security classification, employee use of portable devices, such as cell phones (known as Bring Your Own Device or BYOD policies), and other key areas impacting what and how information is managed.
- *Roadmap* – The committee should be active in the development and review of the overall IG roadmap, including prioritization of projects, timeframes, and ensuring that these roadmaps do not conflict with other existing corporate initiatives.
- *Process Approval* – Review and approval of retention, disposition, discovery, and other IG processes.
- *Technology Review* – Committees often provide input and review of major technology selections, including enterprise content management and archiving systems. While traditionally these decisions are the exclusive domain of IT, the savvy IT organization will realize that allowing this type of input will greater increase adoption of these technologies when it is time to implement them.
- *Training* – Both group coordinator and individual training plans.
- *Internal Communications* – Messaging and communication strategies to business units and employees.
- *Organizational Development* – Once a program is developed, how it will be sustained and who will be responsible for which parts.
- *Milestone Achievement* – Like all successful projects, identifying and reporting on key milestones against the project calendar.

3. Sample Agenda for First Meeting

In-house counsel driving the creation of an IG Committee should carefully plan their first agenda. Lack of an effective IG program clearly causes pain, especially for the legal group, and often the best strategy for in-house counsel, during these meetings, is to let others discuss and realize how these issues impact their own departments. This is an opportunity to build buy in from other groups. Some key questions to be addressed during the first meeting are:

- What pain is being experienced due to too much and unmanaged information?

- Who else should be involved in addressing these pains?
- What should the committee charter be?
- How does the committee create a "plan for a plan" to address these issues?
- What is the committee's timetable?

D.Are We Speaking the Same Language?

It is easy to forget that everyday terms all of us use may not be familiar to people in other disciplines. When someone hears a term they are not familiar with, it is human nature not to admit they do not know what they are taking about. Participants in these group discussions should endeavor to use lay terms and ensure that any special terms used are defined and understood by all.

Legal Vocabulary	IT Vocabulary	Compliance Vocabulary
FRCP & FRE	Active Directory	Whistle Blower
ESI	Fuzzy Logic Searches	FCPA
Legal Hold	BCP	Code of Conduct
Discovery Protocol	Journaling	Control Framework
Custodian of Records	FIPS 199	EU Transparency
Chain of Custody	ASP/ISP	HITECH
Spoliation	Big Data	Red Flag Rule

"I was in a discussion with IT about an archiving system, and they kept talking about fuzzy logic. I didn't know what the heck they were talking about, and quite frankly I tuned out the rest of the conversation" – General Counsel for a large retailer.

III. Developing a Business Case

Sometimes organizations have been through traumatic events, such as a large litigation or a data breach, that clearly exposed their information governance weaknesses, and senior management needs no convincing on the importance of developing and funding a formal IG program. More typical, however, are organizations that, while suffering many of the same weaknesses but having not been through such a watershed event, senior management needs to be convinced these problems need to be addressed. Gaining not only financial but also moral support from senior management for IG initiatives is key to a program's success - they should not be launched without it. Therefore, often the first activity of a newly formed committee is to develop an IG business case for senior management.

There are a number of different strategies for building a business case. The right approach depends in part, on the issues an organization faces, as well as the specific style that senior management prefers when evaluating information.

A. Getting IT, Business Units and Other Key Stakeholders On Board

The first and perhaps hardest part of launching an IG initiative is to build support among other stakeholders. It is not safe to assume that legal's eDiscovery woes, for example, will appeal to HR. Fortunately, effective IG programs provide a win for nearly all stakeholders. Hence, the key to launching these programs is often messaging the win for others.

For example, a sales group may bristle at having their email stored or being expected to properly file their electronic documents. This is the perfect opportunity to suggest ways in which good practices can protect them. Having a complete record of email communication or contract revisions can help to prove ownership of responsibility for a certain promise made to a customer, protecting their relationships and reputations. This same thought process works for many individuals – good records management practices protect their interests just as much as those of the organization as a whole.

Good information governance means that the organization stores less unneeded paper, thereby enabling easier compliance. Retention policies are aplied as appropriate and what is not needed to promote compliance with pertinent legal and regulatory mandates such as those spelled out in the US Federal Rules of Civil Procedue (FRCP), Federal Sentencing Guidelines, HIPAA, ISO Standards, Payment Card Industry (PCI), and DSS is removed.

- *Protecting Sensitive Information* - With guidelines for proper management, it is easier to secure what must be protected, such as personally identifiable information (PII), trade secrets, and other types of corporate confidential data.

- *Reducing Storage and Operational Costs* - IT can centralize the control of information deletion to defer or avoid expenditures and improve application performance.
- *Optimizing eDiscovery* - Control can be asserted over information before the next legal action and repeatable and predictable legal hold processes can be established to minimize business disruption.

Stakeholder	Sample Win and Messaging
Legal	Compliance with corporate retention and destruction policies not only for paper but also email and other electronic documents
Litigation	Significantly reduced eDiscovery risks and costs; narrower legal holds; early case assessment
Privacy	Compliance with EU Data Protection and US privacy requirements; easier implementation of cross border controls; easier implementation of EU "Right to Be Forgotten" requirements
Compliance	Better compliance and monitoring of corporate compliance requirements including FCPA; easier investigations
Records Management	Control, management and disposition of paper as well as electronic information
Risk Management	Better overall controls and reporting for IG-related risks
IP Management	Better collaboration among knowledge workers; easier identification and support for IP development
IT	Reduced data storage costs; better use of existing technologies; better and more useful IT services
Data Governance	Better protection of privacy; higher data quality; avoid "polluting" data lakes
Information Security	Easier identification of corporate confidential, as well as other sensitive information; reduced risk of data breaches
Facilities	Decrease in the amount of paper records storage

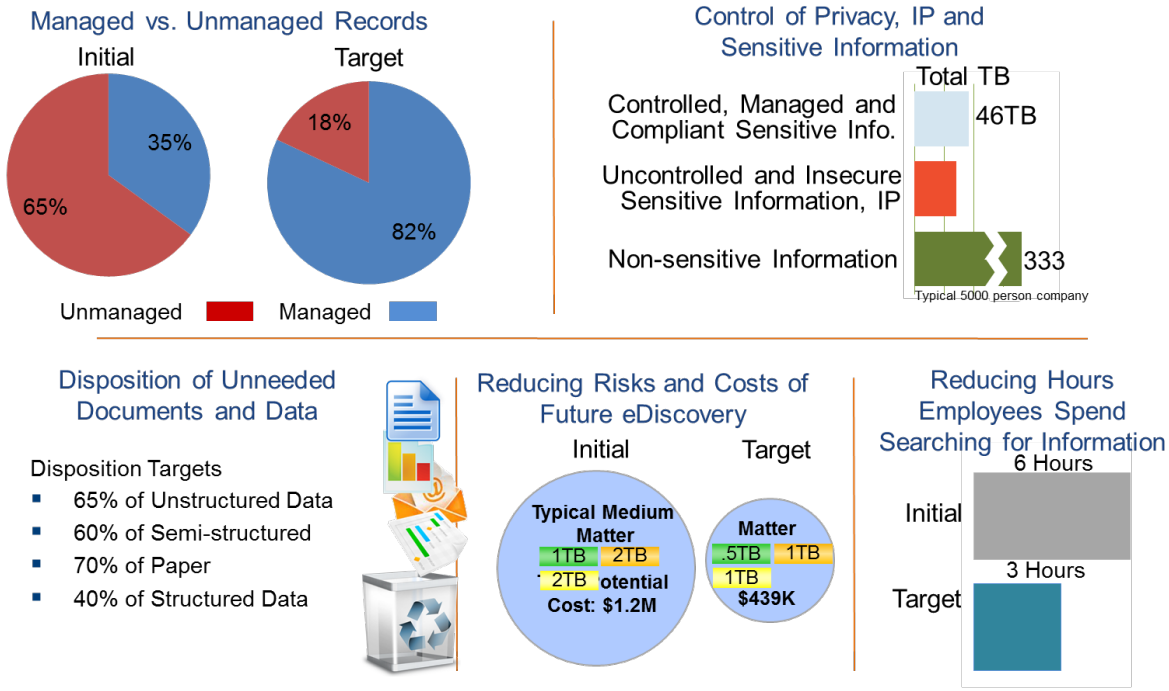
Audit	Better investigation processes; reduced risk of IP breach
HR	Improved collaboration among employees; better management and control against hostile workplace claims
Finance	Potentially large cost savings across multiple groups; better compliance with the Sarbanes–Oxley Act and other regulatory requirements
Business Units	Increased employee productivity; better use and reuse of information; mitigated impact of employee turnover
Individual Employees	Saving an average of two to three hours per week, per employee, searching for information

Sell the program on employee productivity benefits. Records compliance, privacy, and better discovery just come along for the ride. Shared victories also lead to a positive side-effect: functional groups across the organization can develop closer and more trusting working relationships. Each group can rightly claim its role as an enabler of, and not an obstacle to, overall business progress, and the legal department will be viewed as helping drive the business forward.

Perhaps the biggest "win" will derive from better employee productivity and enhanced collaboration. Employees can search and locate what they need to improve their job performance by reducing the time they spend in personal information management (saving and searching for email, files, and other information). In addition, when a project is finished, an employee leaves, or a group is disbanded, information that may otherwise be isolated on desktops or in personal repositories can still be leveraged for future business value.

B. Five Key IG "Wins" for an Organization

Creating a compelling business case often starts with clearly and plainly describing the benefits a program offers. The challenge is that IG is composed of myriad details: specific regulations, for example, or unsecured privacy information on file shares, and higher eDiscovery costs. It is hard to convey the value of these programs without referring to the details, yet senior management tends to glaze over when presented with this detailed, esoteric information.



A more effective approach is to summarize both the problems and benefits of an IG program in five separate areas:

- *Legal and Regulatory Recordkeeping Requirements* – Organizations face literally thousands of regulations requiring them to save, manage, and access records, that exist both in paper and electronic formats. Today, many organizations have a significant percentage of their records that are not identified, classified, or managed, thereby increasingly creating compliance risks.
- *Control of Privacy, IP, and Corporate Confidential Information* – Within their systems, data and documents that are created, received, transmitted, and stored, contain privacy, intellectual property, corporate confidential, and other types of sensitive information. Existing and newer regulations, both domestically and abroad, require organizations to identify, classify, secure, report, and dispose of this sensitive content.
- *eDiscovery Risks and Costs* – Ongoing and continued accumulation of paper and electronic documents both increase the risks and costs of discovery associated with litigation and regulatory inquiry.
- *Defensible Disposition of Legacy Documents and Data* – In addition to the issues identified above, increasing accumulation of information, especially of expired records and documents with little or no business value, continue to overwhelm both paper records storage and electronic storage costs.

- *Reducing Average Hours Employees Spend Searching for Information* – Perhaps the largest impact is on employee productivity. Employees de facto "save everything forever" approaches not only increase the risks above, but also prove a drain on productivity. When everyone has their own individual silo of email, files, and other information, it becomes time consuming to search for valuable content, and increasingly difficult to share and collaborate on this content.

While there are many more than five components to an IG program, almost all aspects can be summarized in the above five areas. Individual programs, such a litigation readiness, can have sub-areas, such as early case assessment, compliant legal hold processes, and data mapping. It is better to describe the program and its impact at a higher level, as often there is too much detail for senior management.

Driver	Impact of an Effective IG Program
Legal and Regulatory Recordkeeping Requirements	Increases compliance with legal and regulatory requirements, especially for electronic information (such as email and electronic documents).
Control of Sensitive Information, such as Privacy, IP, and Corporate Confidential Information	Enables identification, protection, and management of both paper and electronic information, reducing the risks of breaches, meeting emerging privacy rules, better protecting IP, and ensuring appropriate controls and management for confidential information.
Legal Discovery	Proactively setting up policies, processes, and enabling technology to significantly reduce the risks and costs if and when future discovery occurs.
Defensible Disposition	Reduces the amount of older, expired, unneeded, and low-value business information files and documents for both stores of paper documents and electronic information across the enterprise.
Employee Productivity	Classifies, organizes and makes accessible high-business value content for employees thereby increasing productivity, collaboration, and innovation.

Keep it simple, plain spoken, and discuss the outcomes.

C. Finding the Employee Pain

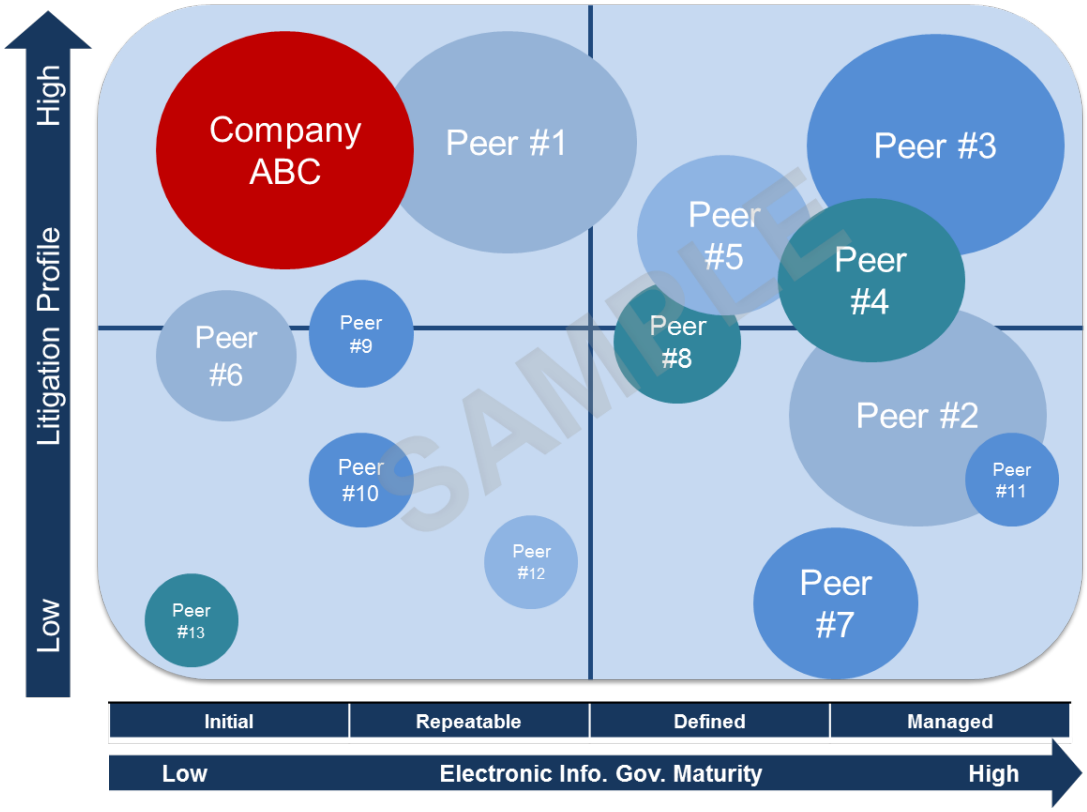
Poor information governance practices certainly can cause pain for legal, IT, and compliance within an organization. As noted above, employees' "save everything forever" practices and other poor practices decidedly drive up legal and compliance risks and costs. Mistakenly, in-house counsel sometimes adopt an "us vs. the employees" thinking that good IG policies and processes will somehow make employees less productive. There is a fear of engaging both employees and business units on these initiatives for fear of creating pushback.

In reality, employees are drowning in information, and interviews often reveal that employees experience significant "latent" IG pain. Some comments include:

- "We are drowning in e-mail."
- "Don't have time to organize."
- "Was on verge of sending out contract when email box full."
- "Every time we reinvent the wheel when I know someone has created this before."
- "I spent five hours updating a spreadsheet last week, only to find out I didn't even have the latest version."

Identify these types of pain within the organization and use it to position the benefits of an IG program. Be able to cite specific examples. Show that IG programs drive better productivity and are not counterproductive. Employee pain is the gasoline that drives the engine of Information Governance.

D. Benchmarking Against Peers in Your Industry



Another effective strategy is to compare capabilities to other peers in the same industry. Senior management wants to know how they compare against peers in their industry. It is somewhat unrealistic to expect senior management to grasp all the details of the program's policies or processes, and an industry benchmark that compares a company's IG maturity against peers in the industry can prove to be a powerful business case.

An industry benchmark is intended to be an approximation of maturity, not a precise measurement. Furthermore, benchmarking can be completed against either an entire program, or just one element, such as litigation readiness. To measure program maturity on a simple scale, information can be collected through a variety of sources:

- Publicly available sources on litigation profiles, such as LexisNexis.
- Discussions with peers at professional societies, such as ACC.
- Informally approaching similar organizations with a simple list of questions.

No single source is likely to provide enough information for a benchmark, and getting a variety of data from different sources will often yield surprisingly useful results. Again, a

benchmark is not meant to be an exact measurement, it is meant to be an approximation of maturity across a range of organizations.

E. Using Return on Investment (ROI) Models to Justify a Program

The financial impact of programs drive many decisions, and senior management tends to prioritize decisions based on financial impact. To address these issues requires organizations to adopt policies and technology and, in doing so, there are associated costs. Organizations turn to Return on Investment (ROI) models to prioritize where they should invest time and money in order to meet their business objectives associated with costs and risks.

An ROI model is a summary of costs associated with implementing these new policies and technologies, which are then compared to the benefits that will accrue in the organization. At a high level, the ROI is a calculation of how much money/risk will be saved in comparison to how much money will be spent. ROI models are traditionally used as a final step in approving projects, and organizations are increasingly using ROI models to help continuously refine programs by using them as feedback mechanisms to ensure the benefits are actually achieved.

ROI models are common for business units and IT to justify their new programs. ROI models are relatively uncommon for corporate counsel and legal teams. That is partially due to the fact that "legal issues" are not well-understood by IT and business units and Legal is typically viewed as an "expense" with little collaboration into ways to improve the underlying needs. This means that IT and the business units are believed to rarely help improve the process or even share ideas that might help address the problem that Legal is trying to address. The result? Many Legal initiatives result in having significant compromises to the goals in order to keep costs low because organizations fail to understand the big picture of benefits that are possible.

Today's progressive Legal groups are incorporating a business view of justifying their projects in much the same ways that the business units and IT have done themselves. They are involving stakeholders across the organization and carefully showing the stakeholders how improvements for a Legal process can actually have disproportionately large benefits when implemented across multiple groups. ROI projects led by Legal are typically more comprehensive than business unit-centric solutions, and also have a greater return on investment. Instead of being a cost center, Legal assumes a role in helping to set business decisions in a comprehensive way that ultimately provides greater benefits than traditional approaches yield.

The advantage of developing an ROI is that it often changes the conversation from "we need to do this because of regulatory requirements" to "we should do this because not only will it allow us to be more compliant, but it will save us money."

There are two main types of ROI models: informal and formal. Informal ROI models collect specific examples, anecdotes, or case studies to build support for a program. Formal ROI models collect detailed cost information for the life of a program, and then project specific cost savings. Informal ROIs are, of course, easier to develop, but may hold less sway with senior management. Formal ROI models, conversely, can be time-consuming to develop, and when done correctly make a persuasive argument. The right approach for any organization depends on the management culture of that organization.

1. Creating an Informal ROI

An informal ROI presents the costs and potential savings for one or several aspects of an IG program. These are often presented as case studies or risk profiles as part of a business case. They do not attempt, however, to fully quantify all of the costs, risks, and savings.

Some guidelines when developing an informal ROI include:

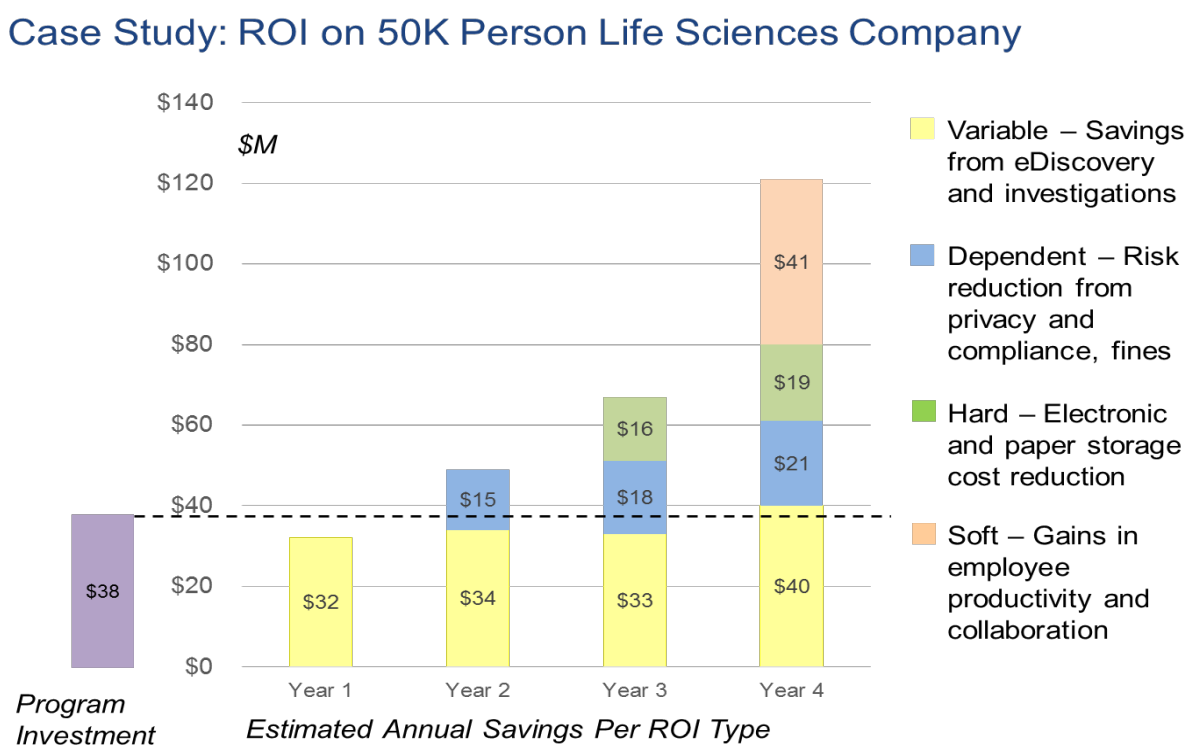
- *Use Specific Examples* - Show the actual costs of eDiscovery, the costs a similar company incurs when addressing a data breach, or the amount of productivity hours lost due to poor information management when an employee retires.
- *Exact Dollar Figures Are Not Needed* - It is acceptable to provide a range of savings, especially for informal ROIs.
- *Use Examples from a Variety of Areas* – Use examples from other areas, not just legal.
- *Length of Time* - Do not assume that a high litigation profile, for example, will continue into the next two years. Likewise, do not assume that because a company has not experienced significant litigation in the past three years that it will not occur next year.
- *Interconnectedness* - Be sure to demonstrate the interconnectedness of Information Governance, and speak to how a proper program can address the root cause of these issues, not just the symptoms.

Some examples of informal ROI case studies include:

Sample Informal ROI Case Studies
"During a recent class action litigation, Company ABC spent $1.1M on eDiscovery with an outside vendor. Many of the documents and files turned over to the eDiscovery vendor were older, unneeded and sometimes duplicative copies pulled

from file shares and other unmanaged repositories. There are currently no processes for identifying and classifying active records from older information. Our eDiscovery costs for this case was likely 2X what it could have been had we had a program in place."
"Our competitor Company XYZ recently suffered a data breach. The perpetrators had access to a home-grown database on an employee's desktop computer containing customer emails and other information. Company XYZ is going through a breach notification process. We believe our company may also be subject to the same types of risks."
"A recent audit found that we had highly confidential process design documents living relatively unprotected on our file systems and email server. It would be relatively easy for an outside hacker or a disgruntled internal employee to collect a relatively large cache of these documents, putting our trade secrets at risk."
"Our company recently received a regulatory inquiry from the Federal Trade Commission on how we price one of our products in a few states. It took us a while to locate, review, and produce the information they requested. As a matter of fact, it took too long, and they believed we were stalling so they significantly increased the scope of the investigation. The original inquiry was relatively small, but the new expanded inquiry is much larger and likely to be much more expensive."

Note that for most organizations it is not typical that a single case study will carry enough weight to drive the adoption of a single program. What does work is providing multiple different cross-functional examples, each adding weight to the need of a program, and collectively all of them tipping the scale toward adoption.



2. Creating a Formal ROI

Legal departments are unique in an organization in that they usually have the most visibility to the biggest issues affecting the organization. Whether it be risks for new regulations or lawsuits or understanding of the macro business drivers affecting new products and reporting to shareholders, senior legal counsel in an organization can play a vital role in helping to see the big picture that can be more difficult for those focused on running the day-to-day aspects of the business.

Because of this, Legal is often best suited to drive the big picture for ROI and understanding the areas where justification can be found. There are five key areas:

- *Data and Document Storage Costs* - For most organizations, their data and documents are growing at a faster rate than their underlying business. In almost every organization, these costs are significant and frequently under-reported. The vast volumes of information mean that ever-increasingly complex processes and systems must be put in place to deal with them. If not, processes will evolve that ignore data that would otherwise be useful in business decisions but must be ignored because it is too difficult to find. Data and documents can generally be classified into the following content categories:

- *Structured Data* - Data that is in a database and often used in a line-of-business application. Increasingly includes data stored in third party cloud solutions.
- *Semi-Structured* - Unstructured information that has a database containing some information about the document or message. Document management systems and most SharePoint implementations are semi-structured.
- *Unstructured* - Documents that do not have associated metadata (file properties do not count). The most common are shared drives and documents stored on personal computers.
- *Messaging* - Includes email and instant messages.
- *Video/Audio* - Includes voice mails and other video and audio that may be produced in the course of business operations. These volumes are usually low in comparison to the other content categories, and they are especially difficult to manage and process in eDiscovery situations. Voice messages on cell phones owned by individuals (but used for company business) are also included and especially problematic.
- *Paper* - Includes paper records with off-site vendors as well as stored internally (i.e., on site).
- *Backup* - Backup data, including tapes and virtual tape libraries.

Each of these content types has different characteristics in terms of costs, accessibility, and technology choices to affect the data.

■ *Litigation Costs and Risks* - No one in an organization is more qualified to address the costs and risks associated with litigation than the legal department. (For purposes of this discussion, litigation includes efforts related to regulators or similar outside parties.) There are two components to all litigation: the cost of the litigation itself and the risk associated in terms of judgments, fines, etc. On the cost side, a good ROI counts the number of small, medium, and large matters and makes estimates of those over time. Each of these is broken into how much content is typical based on the seven content types described above. Finally, the costs are broken into Internal Collection, Processing (Vendor Review), Legal Review, Vendor Production, and Legal Production. Most do not include attorneys' costs for the "legal activities", although some organizations feel that they have higher litigation spending specifically because of current poor processes, and could include some percentage of those in a reasonable model. Risks are calculated based on the impact of each litigation event, including a weighted average of the cases. For example, if 20 "slip and fall" cases per year are anticipated with average settlement of $15,000, the total risk would be $300,000 per year. If the new processes and systems can make it easier to litigate cost effectively, an assumption might be that the average case can be settled for $12,000 or $240,000 per year. In this scenario, the risk reduction would be $60,000 per year. These types of analysis are best used in a conservative fashion

because this type of analysis is not common in an organization for the business units other than Legal. Outside assistance and review of the assumptions can often find additional savings but also make the assumptions easier to defend because of prior expertise.

- *Breach for Intellectual Property and Privacy* - This is one of the least understood areas of ROI, and also has high levels of return and can often be relatively easy to address. This is another type of risk and must be weighted like the Litigation Risk described above. Privacy, in particular, is becoming more important and can be especially problematic for multi-national organizations. The multi-jurisdictional requirements are especially challenging for lawyers who are typically only aware of the rules in their home country. For example, the act of transferring an HR record from Singapore to the U.S. may be in violation of the Personal Data Protection Act and includes fines up to $820,000 USD if such information can result in "hurt feelings." Europe has a variety of privacy standards that are complex and difficult to navigate. These same issues are at play for intellectual property. The Sony data breach effects in 2014 could have been minimized with better records management policies, content segmentation, and improved detection procedures. Losses of intellectual property to competitors and customers can have tremendous impacts.
- *Transborder Data Flow Regulations* -- Some business data in Europe may not be stored or moved in the U.S., while other types of data can be moved and still others can be moved temporarily, if certain conditions are met. Russia and other countries have new rules that require copies of data to be kept on servers within their countries, while some require that the data never leave the country or region. Like HIPAA, the fines can be based on the number of records improperly moved so the fines and legal settlements can be quite significant.
- *Employee Productivity and Collaboration* - Most ROI models focus on employee productivity, especially for user-focused systems (such as ECM and SharePoint) where large numbers of users can share and collaborate. These savings can be significant. ROI models that exclusively use just Employee Productivity can often justify entire multi-million dollar projects in 24-36 months. One problem is that these models often are theoretical and include partial full-time employee productivity that does not translate to real-world savings. For example, if the system is projected to save a person 15 minutes per day, that can represent a substantial hard dollar savings when applied to thousands of workers. That savings, however, is only theoretical and is not actually realized unless the workers can be redirected or if people can be removed from that function because there are enough people that entire positions can be eliminated.

3. Avoiding Common ROI Mistakes

ROI models and cost justifications are nothing new, but the failure rate is still very high. Most people can recall an expensive project or two that failed to meet the business objectives. In extreme situations, organizations have had to scrap their systems and start from the very beginning again. Sometimes, these failures are from systems not working properly or poor project management, but often, the failure occurs from the very beginning of building the justification.

Some common mistakes include:

- *Not Addressing the Real Problem* - One hallmark of traditional western management culture is that it tends to reward quick solutions. This is especially true in American businesses where fast-thinking and fast-acting leaders are celebrated as pop-culture icons, even if the original ideas failed. This approach means that organizations often look for "technology insertion" opportunities based on an almost religious view that adding technology will improve the business. From websites to phone systems to matter management systems, the assumption is that adding technology will automatically be a good thing and yield praise-worthy benefits. Smart organizations focus on the business problem first and then only apply as much technology as is absolutely necessary to achieve the maximum benefits. This approach means targeted and often more-limited solutions that are laser-focused on cost effectively finding the information needed to address risk.
- *Incomplete View of Current Costs* - ROI models are notorious for over-estimating savings. Ironically, many business units are especially skeptical of Legal when it comes to making assumptions about their business operations. For buy-in purposes, it is important that Legal work closely with the business units to get buy-in throughout the project, and especially so on understanding the underlying cost structures. One major problem is that most organizations assume the money in a budget for a particular operation reflects the true cost to the organization. In most cases, that is false. Budgets are designed to track how costs are allocated and while they have some relationship to costs, they are imprecise and only reflect how the costs are summarized, not how money is actually spent. Consider, for example, the salary of an insurance clerk. The budget for the department only assumes the cost of the person for their salary, benefits, and office supplies. But to do their job, they also require the use of computer software and they need to have managers and HR support – costs that appear in different budgets. One of the hardest aspects of any ROI model is developing a current cost model that is accurate, as it is absolutely critical since that forms the basis of all decision-making from the model.
- *Optimistic Expectations of Future Costs* - Everyone is familiar with projects that run over-budget during the initial implementation, yet the bigger problem is when the operating costs are higher than expected. Some suppliers to the Legal community have entire business models based on setting an expectation of a low

initial cost when they know they will increase their profits with required add-ons and additional fees and services that are not readily apparent. Even internal costs are often under-estimated, thereby inflating the reported ROI. For example, the vendor may sell a software search tool that is used to search for records for eDiscovery purposes. The team believes that they only need to buy the system and then pay the software maintenance charge. In reality, a part-time IT person is needed to do security administration and run back-up processes. On top of that, the search tool requires specialized tuning that requires expensive professional services from the vendor in order to make it work. In some cases, these types of hidden operating costs can quickly exceed the entire purchase and implementation of the initial system.

- *"Subsidizing" Features that are not Cost Effective on Their Own Merits* – Getting approval for new technology or funding for additional people can be difficult. Human nature means that people look for opportunities to "bundle" what they want into a request that is likely to be approved. In some organizations (and especially in government) there are sophisticated cultures that rely on this approach in order to get things done. The problem is that this distorts the ROI calculations and can fundamentally lead to poor business decisions. Consider a team choosing between Solution A and Solution B. Solution A is the less expensive solution and the ROI model calculates that it will pay for itself in three years, well within the five-year cut-off that senior management uses to approve projects. But Solution B has some features that the evaluation team really likes, even though it is more expensive. The ROI model calculates that Solution B will pay for itself within four years, still within the five-year cutoff. The team selects Solution B because they can still get it funded and they like the additional features. However, this is the wrong approach. Solution A should be considered the "baseline." It solves the business problem with the maximum return on investment. For Solution B to be better, the additional features themselves should improve the cost justification. As it turns out, those additional features are nice to have, but they do not generate enough additional savings to be cost-justified. Selecting Solution B lowers the return and, therefore, is not the best solution.

F. Presenting Your IG Business Case to Senior Management

At some point, the steering committee will be asked to make a business case for senior management. Some successful approaches include:

- *Approach Management as a Committee* – It is not a single group. This will add significant weight to the proposal.
- *Don't Weigh Too Heavily on Compliance Requirements* - Management may end up thinking Yes, compliance is required, but management may assume that they've gone this far without it, is it really needed now?

- *Information Governance is Not Inherrently Complex* - Keep descriptions simple and avoid buzzwords.
- *Demonstrate How the Proposed Strategy is "Right-Sized" for the Organization and Culture* - Show how, in many cases, a "Chevy" instead of a "Cadillac" approach has been taken.
- *Present the Initiative in Phases* - Include clear completion criteria at the end of each phase, and a go/no-go at the end of each phase. Keep a bigger picture view of what needs to be accomplished over a longer period of time, which will reduce the risk of programs stalling out.
- *Successful Program Communications* - Include how a successful program not only aids records and eDiscovery, but also other corporate initiatives, such as FCPA and data governance.
- *Be Upfront About Program Costs* - Include internal resources, capital expenditures of technology as well as outside services and indicate on the timeline when the company is likely to incur these costs.
- *Use Actual Examples* – Include real-world examples of privacy data found on a public file share, the impact of when an employee had the wrong version of a document, or historical eDiscovery costs.
- *Set Target Metrics* - (see Section V) Set proper metrics and commit to providing updates on the successes of meeting those metrics.
- *Employee productivty* – Employee productivity and reducing the impact of turnover is a key "money slide." This is the driver most likely to carry the day.
- *Ask List* - Be clear in the IG "ask list."
- *Conclude with the Big Picture View* - Poor IG practices can tie down and hold a business back. Good IG practices enable the employees to be more productive and the business more agile.

Because of the nature of today's businesses, senior managers are forced to have different priorities and ways of looking at the business to address more immediate concerns. For example, an organization facing a high amount of litigation may focus on driving eDiscovery costs down while another might focus on solving long-term issues to reduce the liability in the first place (especially if they think the litigation is likely to grow). For almost every organization, operational cost savings are still critical.

IV. Creating an Information Governance Roadmap

Often the most difficult part of an IG program is simply getting started. Even with key stakeholders involved and senior management support, IG steering committees wrestle with a number of questions:

- What's the right size program for the organization?
- What projects should be included?
- In what order should the projects be executed?
- How long will it take?
- Can existing technologies be used or do new systems need to be purchased?
- How much will it cost?
- How much will it save?

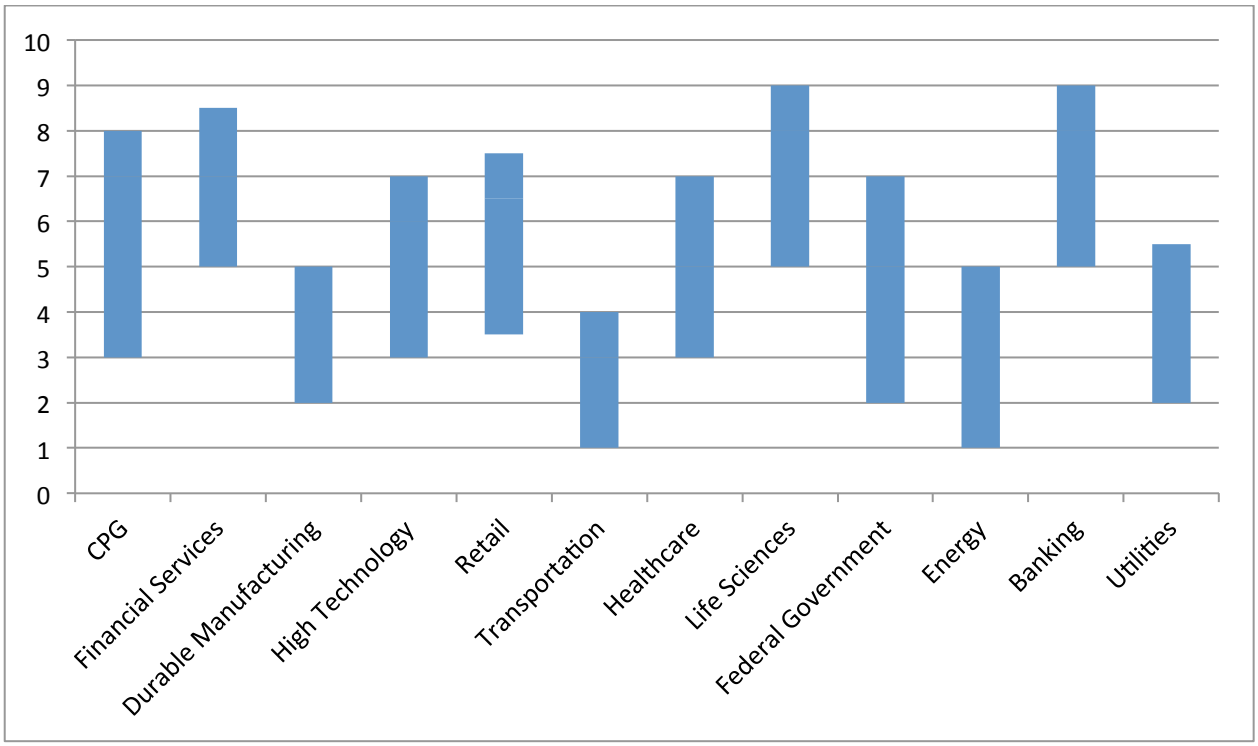
These and other questions are best addressed through developing an IG roadmap.

A. Take a Divide and Conquer Approach with Wins along the Way

There is a tendency to simply start with a small component and work on that, without worrying about some of the bigger picture details. But even small initiatives run across, and may conflict with, other program elements. Organizations wanting to dispose of files and other unwanted unstructured data, for example, may start with an electronic data deletion project. But before this can be done the records retention schedule may need to be updated. Then someone realizes that the legal hold process should be addressed so information under legal hold is not deleted. Just getting started can be difficult. Avoid creating one single, large project. Rather, to avoid getting stuck, take a big picture view and develop a roadmap that divides projects into smaller, more manageable pieces.

As the strategy is being developed, consider the timeline in which these projects can be completed. The timeline should factor in competing initiatives, funding, and the speed at which the organization can absorb change. Some smaller programs can be executed in a quarter or two. Larger and more complex organizations often have IG program timelines that may span a number of years. Perhaps most important, each project or small group of projects should offer an organizational "win" in which the enterprise witnesses the benefits of these types of programs. Having wins early and then throughout the process will help build momentum and buy-in, as opposed to experiencing a win at the end of a series of long projects.

B. Sports Car, Sedan or Golf Cart – Picking Your Program Maturity



Organizations should consciously target the appropriate level of maturity for their IG program. Technology vendors and law firms often warn of dire consequences of poor IG efforts (and that only their technology or services will avoid these disasters.) In reality, organizations have a wide range of compliance requirements, litigation profiles, privacy risks, cultures, and resources available. A few organizations do indeed need a "sports car" level of program maturity; however, more organizations would be better off with a "sedan" or even "golf cart" level program. It is better to have a well-executed, albeit simpler, approach than a more complex, difficult, and expensive "sports car" target maturity that spends more time in the repair shop than being driven. Senior managers know this to be the case and savvy IG professionals know that targeting the right level of maturity is key.

Take note that maturity varies tremendously across industries. Industries facing more regulatory requirements or higher litigation profiles in general have higher average information governance maturity than those in less regulated industries such as manufacturing. Often senior management is willing to invest in a target maturity level that is slightly above the average in their industry, but are less interested in having a program that is far above this. This is OK, so long as maturity is properly calibrated.

Make a conscious choice on target maturity based on these factors. When justifying a program, be sure to explain the choice and the rationale behind it.

C. Outside IG Frameworks and Standards

Sometimes organizations want to refer to outside IG frameworks and standards to gauge target program maturity. Some of these standards include:

Outside IG Frameworks and Standards	
Records Management ▪ Legal and Regulatory Requirements (10K+) ▪ Generally Accepted Recordkeeping Principles (GARP) ▪ Information Governance Maturity Model (IGMM) ▪ Federal Sentencing Guidelines ▪ EDRM Information Governance Model ▪ ISO 15489-1:2001	**eDiscovery** ▪ Sedona ▪ Sedona Canada ▪ EDRM.net ▪ Case Law (Pension Committee v. Bank of America, Victor Stanley v. Creative Pipe, Chin v. Port Authority) ▪ TREC ▪ Practice Direction 31B (UK)
Information Security ▪ FIPS 199 ▪ ISO 27001, 27002 ▪ HIPAA ▪ General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 ▪ Privacy Shield ▪ PCI Requirements ▪ State Privacy Laws ▪ GLBA	**Data Storage and IT** ▪ ITIL ▪ ISO 32000-1 (PDF) ▪ CORBA

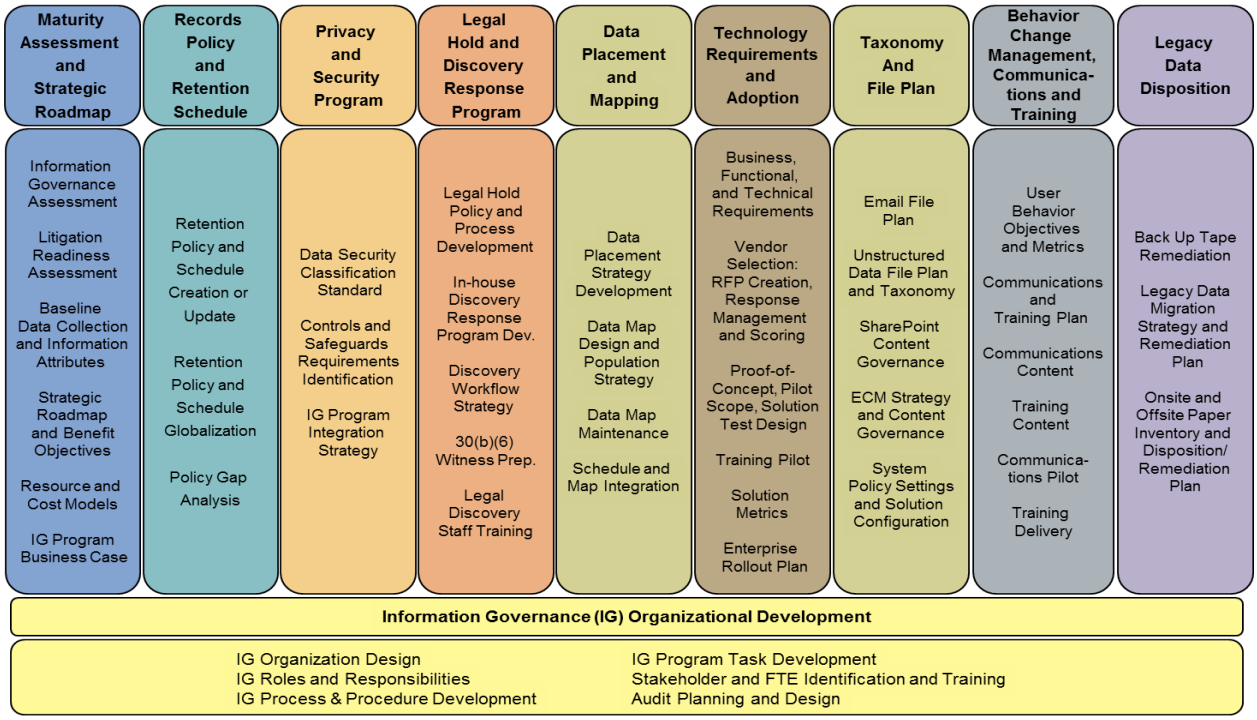
These multiple standards create some challenges:

- Many of the above are only focused on one small piece of IG, such as eDiscovery. No standard or framework addresses all of IG.
- Some are well-defined standards and most are less prescriptive frameworks. IGMM, for example, is at best a framework. It does not provide much prescription on targeting specific levels of maturity.
- Few of these provide any type of objective measurement against current capability.

The above standards are useful in examining program elements, such as FIPS 199 for information security. As of today, however, no single standard exists for an overall IG

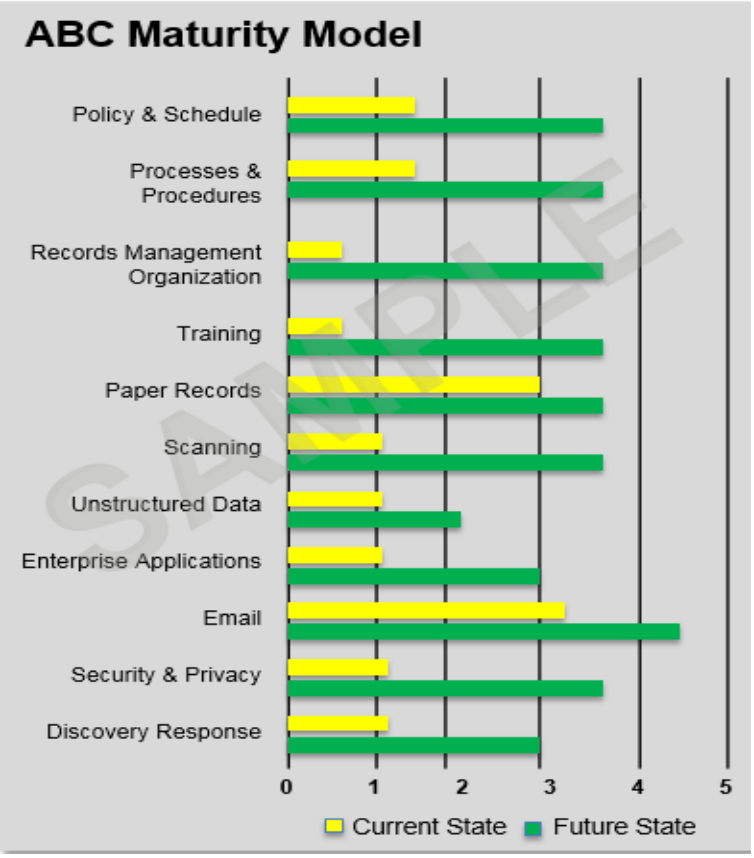
program (and one is not likely to come around in the near future). As a result, organizations often assess their own needs based on a variety of drivers, as well as against peers in their own industry.

D. Assessing Current State and Developing a Roadmap



Since the process must begin somewhere, an IG assessment is a good place to start. Before figuring out where to go, a comprehensive understanding of where the current state and how it materialized is needed. This helps when determining where to be in the future.

Even if the general counsel knows, or thinks they know, that the current program is weak, or that the program needs some improvement in certain areas, an IG assessment is key to help identify what truly does need improvement, what steps need to be taken to effect the improvement, and who needs to be included in each of the steps. The assessment will help to identify the weak areas and confirm the slightly stronger areas. Skipping an IG assessment is like jumping into a lake without knowing what is in it. Issues or employee pain points cannot be properly identified without conducting a thorough assessment.



An IG assessment will provide a holistic, enterprise-wide perspective so that an organization can develop an approach to viewing information as a strategic asset that can support organizational objectives. The assessment can be benchmarked against other organizations in the same industry or organizations of the same size or revenue. This will help determine where the organization's profile sits – what gaps are acceptable and what needs to be bridged to get to the desired future state.

An IG assessment will take into account the organization's culture, risk and litigation profile, operational environment, appetite for maintaining a program, user behaviors, and existing infrastructure. One important goal of an assessment is to understand the business needs and actual behavior patterns of employees who create, manage, and destroy records in all formats (paper, electronic and other physical formats). This helps an organization prevent costly mistakes that can occur when organization's jump into technology solutions without having a good understanding of the business requirements. It also helps an organization formulate a comprehensive program that responds to all the important business drivers – not just a narrow view from one functional perspective.

	Recommendation	Priority	Effort (XYZ)	Cost
1	Update/Simplify Policy, Schedule and Procedures to Incorporate Electronic Records Management	High	Medium	$$
2	Enhance Records Management Organization and Matrix of Records Coordinators	High	Medium	$-$$
3	Develop Email Management Strategy and Solution Requirements	High	Medium	$$$
4	Develop RIM Behavioral Change Management Strategy, Content Creation and Delivery Vehicles	High	High	$$-$$$
5	Unstructured Electronic Data Placement/Management Strategy	High	Low	$$
5a	File Share Clean Up/Offices and Centers File Plan Development/Training	High	High	$-$$
5b	Develop Enterprise Content Governance/s File Plan Dev./Training	High	High	$$-$$$$
5c	Develop Authenticated Electronic Signature Process	Medium	Low	$-$$
6	Evaluate and Implement Enterprise Search Solution	High	Medium	$-$$
7	Legacy Structured Data Strategy and Remediation	High	Medium	$$-$$$$

8	Security & Privacy Improvements	High	Medium	$-$$$
9	Enhance Litigation Tools and Training	Medium	Low	$
10	Standardize Scanning Guidelines and Processes	Medium	Low	$-$$
11	Develop Integrated Content Data Map for Electronic Information	Medium	High	$-$$
12	Update Desktop Backup Solution	Medium	Low	$$-$$$

Information gleaned from the assessment can then be used to create a strategic roadmap that addresses the gaps and provides steps to achieve the desired level of records management, litigation readiness, and the protection of sensitive information. The roadmap provides a clear, detailed project plan for executing the overall IG initiative.

E. Developing a Records Policy and Retention Schedule

Both the records policy and records retention schedule (RRS) are the cornerstone of an effective IG program. They provide guidance on the application of existing laws and regulations, and can significantly ease and accelerate downstream execution.

A records policy is the "what" of the program, whereas the procedures are the "how." The policy should cover records management objectives, scope, definitions, and guidelines, including legal hold obligations and the consolidation of existing policies enterprise-wide. A policy should also make clear why the organization needs a records management policy and the types of records to be covered. The policy speaks in terms regarding retention periods, security, privacy, and storage of records. It should also indicate whether electronic data, such as email, instant messages, and content generated from social media and collaboration tools – as well as drafts and convenience copies – are to be considered business records. The policy also needs to include the specific roles and responsibilities of the records management staff, legal department, other employees, and outside personnel who handle organizational records. The policy must also document provisions for violations of the policy.

A well-designed RRS will be compliant and defensible and will address applicable audit and legal considerations, including specific business and operational requirements. The RRS ensures compliance with federal, state, and industry-specific, as well as country-specific international record mandates. The RRS should include minimum retention periods, retention trigger events, applicable laws and regulations, and descriptions of the records (paper/physical and electronic) that the organization maintains in the regular course of business.

Whether an organization has an RRS that needs to be updated, or one that needs to be created, the RRS should:

- Reflect the full range of all records (regardless of media),
- Be organized into categories/classes that represent all business units, include selected examples for each record category/case (to enhance end-user understanding of the meaning and scope of each category/case), and
- Reflect the business value of records.

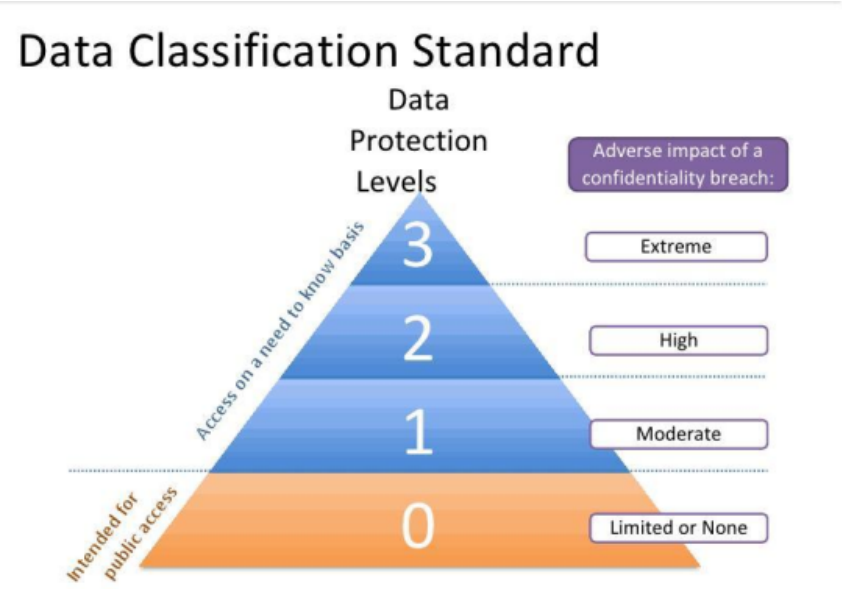
These are attributes of a well-designed RRS, and they will ensure the simplicity of:

- Implementation
- Usability and adoption
- Training
- Compliance

See Section VI (Record Retention Policies and Schedules) for a more comprehensive discussion.

F. IG to Drive Privacy and Security

Increasingly, more organizations are putting data privacy and security classification into their IG programs for electronic records and information, as well as paper/physical. Organizations have, for example, confidential information, financial information, privacy information, intellectual property and trade secrets, and data protection requirements. Having a comprehensive, integrated data security classification policy and strategy that conform to RIM and privacy program objectives, and are comprehensive and easy to follow, is often a critical component of an organization's IG program.

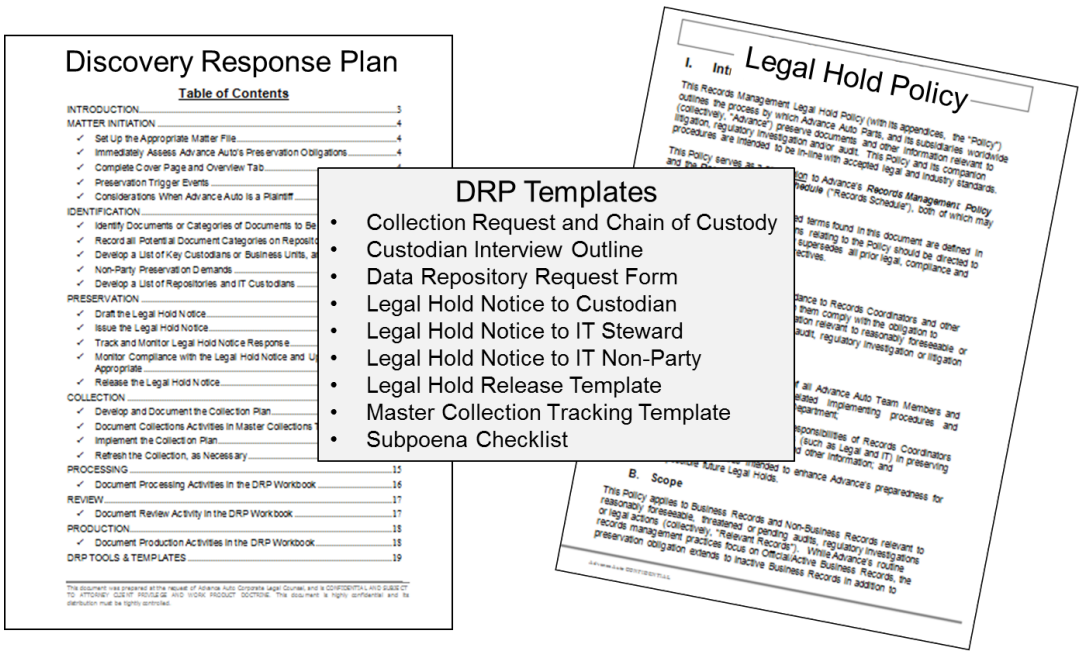


Organizations are beginning to tie their records management activities to their data security and privacy. Organizations need to develop a detailed analysis of the flow of private, sensitive, personally identifiable information (PII), and evaluate the effectiveness of existing controls with respect to applicable internal policies and external regulations. From that analysis, a standard framework for classification of information and documents, in terms of levels of sensitivity or security (such as Public, Internal Use Only, and Confidential) can then be developed.

By including privacy and security into the IG program, organizations are putting steps in place to minimize data breaches and misuses of sensitive or critical information, which in turn improves user compliance through steam-lined and easy to understand categorizations.

G. Developing a Formal Legal Hold and Discovery Response Program

Many organizations are updating their legal hold policies to incorporate eDiscovery response processes; that is, processes to address electronic information, not just paper and physical records and other information. To do so, they must take a step back, get away from their lawsuit specific activities, and look at what can be done to improve their litigation readiness profile. They need to look at it from a higher level. For example, organizations must look at what can be done around creating new policies and putting new processes in place so that when litigation strikes (or is anticipated), it is less risky, less expensive, includes less burdensome procedures, and is more compliant.



This approach includes creating repeatable, defensible processes for how the organization manages and responds to requests for information regardless of location or format. Prior to any anticipated or actual litigation, organizations must set up effective hold processes that address the following requirements:

- *Hold notification* – The issuance of a litigation hold notice that lets custodians (employees as well as non-employees, as applicable) know of their obligation to preserve relevant information, and specifies how they should do so.
- *Information security* – To prevent the deletion, loss, or inaccessibility of relevant documents, such information needs to be saved in a repository that is separate from other information assets.
- *Ongoing preservation* – A process must be put in place to ensure that once a hold notice is served, all future relevant documents are also subject to the legal hold and are properly preserved.
- *Hold release* – Once a particular matter has been settled, and provided that future litigation is not anticipated, the organization should "release" the hold, notify custodians, and resume normal retention and disposition programs.

All of these elements of the legal hold process must be supported by documented procedures, standard templates, repeatable workflows, and forms (or electronic tracking and management systems), along with the appropriate training for litigation support staff, organization managers, and all other employees. By developing an IG program inclusive of a legal hold policy that includes eDiscovery protocols, organizations will be better prepared to address lawsuits as well as any legal or regulatory changes that may occur.

H. Creating a Data Placement and Mapping

Organizations need to develop strategies for saving the right information in the appropriate repositories, referred to as a data placement strategy (DPS). This type of strategy determines where data and documents should live based on their privacy, security, intellectual property, collaboration, discovery, and retention requirements.

The strategic plan needs to be created that documents how various repositories will be used with each other to accomplish specific sets of business requirements, designed to layout the flow of information from initial receipt or creation by employees through the stages of authoring, collaboration, retention, and disposition. This DPS should outline the overall approach to take in the placement and management of all electronic data.

In order to develop a DPS, organizations need to conduct a data mapping. This will allow them to identify what data they have, where it resides, who owns the data, and who uses the data. The result of preparing a data mapping is that it identifies:

- A list and general description of relevant systems, including the nature, location, storage size, organization, and formats employed in each.
- Any limitations to the accessibility of information as electronic documents of limited accessibility may include those created or used by electronic media no longer in use, maintained in redundant electronic storage media, or for which retrieval involves substantial cost.
- Metadata, such as age, owner, date of last access, and keywords associated with relevant information.
- A list of the most likely custodians of relevant electronic materials, including a brief description of each custodian's title and responsibilities.
- The name of the individual responsible for electronic document retention policies (typically the records manager or coordinator), as well as a general description of the electronic document retention policies for the systems identified above.

After conducting the data mapping, many organizations then realize they have a lot of information where it should not be, including sensitive information, records not controlled, documents on hard drives and file shares, and documents on mobile devices. This is another justification for utilizing a data placement strategy – a very important part of the IG roadmap.

The DPS document should include descriptions of strategic goals, objectives, roles and responsibilities, governance and usage guidelines for repositories involved in the overall strategy, including end-user desktops, file shares, email, and other potential unstructured repositories for user-created electronic data. It should also take into consideration existing infrastructure, and may also include previously purchased but not deployed components,

upgraded versions of some software and infrastructure, and placeholders for specific technology solutions yet to be identified.

By embarking on a DPS and developing a data mapping document, the organization is providing a full governance framework, simpler user experience, increased compliance and collaboration, simplified taxonomy development, and reducing the amount of data not placed in appropriate repositories. These processes support the development of appropriate repository usage protocols, centralization of records, and information governance with distributed management across all repositories, resulting in reduced storage costs, reduced discovery cost and risk, and increased coworker efficiency and productivity. These processes also allow the appropriate protection to be applied to information and repositories that require it.

I. Defining Technology Requirements and Adoption

Having completed the above steps to building an IG roadmap provides an organization the opportunity to now make some decisions around technology. Many organizations take the approach of looking at technology first. This is not a wise approach. It is better to do it later in the process, as the requirements your data and documents have is now known. This is an excellent time to select the right technology. Once an organization understands its business, compliance, and legal needs, it will be much more informed, be able to make better decisions, and get much greater use out of its overall technology solution and environment.

	Score			Score			Score			Score			Score			Score		
Categories	Score	Weighted Scores		Score	Weighted Score		Score	Weighted Score		Score	Weighted Score		Score	Weighted Score		Score	Weighted Score	
Administration & Management Capabilities	107		5.35	126		6.30	88		4.40	89		4.45	96		4.80	113		5.65
eDiscovery	413	94.25	14.14	412	97.15	14.57	229	55.10	8.27	267	62.95	9.44	340	78.75	11.81	195	53.85	8.08
General	25	2.50		15	1.50		23	2.30		17	1.70		18	1.80		10	1.00	
Identification	80	24.00		105	31.50		64	19.20		69	20.70		71	21.30		74	22.20	
Preservation	65	19.50		65	19.50		45	13.50		41	12.30		54	16.20		58	17.40	
Collection	53	13.25		45	11.25		36	9.00		47	11.75		45	11.25		53	13.25	
Processing	55	11.00		55	11.00		29	5.80		29	5.80		51	10.20		-	-	
Review	105	21.00		97	19.40		21	4.20		43	8.60		79	15.80		-	-	
Production	30	3.00		30	3.00		11	1.10		21	2.10		22	2.20		-	-	
Email Archiving	114	31.20	5.46	160	44.00	7.70	110	29.80	5.22	121	34.70	6.07	148	41.40	7.25	133	36.90	6.46
Archiving	21	6.30		45	13.50		29	8.70		27	8.10		40	12.00		43	12.90	
Capture	43	12.90		55	16.50		37	11.10		46	13.80		53	15.90		35	10.50	
Indexing	35	10.50		40	12.00		28	8.40		40	12.00		40	12.00		40	12.00	
PST Ingestion	15	1.50		20	2.00		16	1.60		8	0.80		15	1.50		15	1.50	
Technical Solution	87		15.23	107		18.73	96		16.80	70		12.25	87		15.23	87		15.23
Usability and Learnability	39	21.20	6.36	48	25.80	7.74	38	19.80	5.94	37	20.20	6.06	43	23.80	7.14	37	20.00	6.00
Client Access Features	28	16.80		33	19.80		23	13.80		27	16.20		33	19.80		26	15.60	
User Interface	11	4.40		15	6.00		15	6.00		10	4.00		10	4.00		11	4.40	
Retention Management	77	22.90	3.44	101	30.40	4.56	69	19.40	2.91	26	7.90	1.19	87	26.20	3.93	21	6.40	0.96
Audit & Monitoring	12	6.00		18	9.00		6	3.00		5	2.50		16	8.00		4	2.00	
Classification	39	11.70		48	14.40		38	11.40		12	3.60		40	12.00		10	3.00	
Policy Management	26	5.20		35	7.00		25	5.00		9	1.80		31	6.20		7	1.40	
TOTALS	837		49.97	954		59.60	630		43.53	610		39.46	801		50.15	586		42.37

At this point in the roadmap, an organization can drive the development of specifications by understanding current challenges, existing processes and desired business outcomes, which in turn, will drive the development of clear functional requirements (what a system is supposed to accomplish from a business standpoint) and technical requirements (how the system works, its architecture and design). Organizations should start with a thorough analysis of business challenges, regulatory pressures, processes, and software systems currently in place. Detailed interviews with key stakeholders (e.g., business units, legal,

and IT departments) can uncover assumptions, expectations, business needs, desired outcomes and specific use cases. Each requirement needs to be documented and include a brief summary and rationale as to why it is important. All requirements should then be documented in a clear and readable format that ensures everyone is on the same page.

If it is determined that new technology is needed, or that existing technology needs updating, functional and technical requirements can be documented that can inform possible suppliers as to what the solution must do, who will use it, and how it will be used. From this, a Request for Proposal (RFP) can be developed so that the organization can objectively compare the features and benefits of competitive solutions.

After selecting the preferred solution, an organization should then plan and execute a Proof of Concept (POC) and Pilot testing periods. The POC is primarily a set of unit tests and some integrated tests, as needed, to show that the features and functionality of the technology solution are working and acceptable to the core team (typically IT and Legal/Compliance). The Pilot testing period is primarily about the end user experience. It covers messaging, training, user productivity and behavior, on-line self-help tools, helpdesk support (both in IT and Legal), and the rollout process. This activity is designed to test the entire solution (policy, technology, and people), not just the technology itself.

At the end of these exercises, an organization will have a functioning solution that meets its requirements, has been tested for performance (works as advertised), and has been tested by a group of key internal users who can provide valuable feedback for making adjustments before enterprise-wide rollout.

J. Developing Taxonomy and File Plan

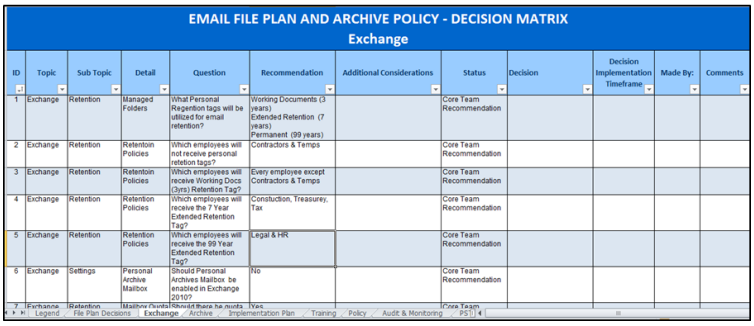
Now that the data has been identified and mapped, a standardized, organizational structure needs to be developed to ensure proper management of all that information. An organization needs to develop a hierarchical structure for organizing documents and associated metadata so that the information can be properly and consistently classified, making it readily available for retrieval as needed.

Perhaps an organization has moved to Office 365, or SharePoint, or some other ECM solution, or is implementing an updated email environment. In any of these scenarios, several concerns must be addressed, such as how:

- The solution is set up so that it matches the DPS.
- The solution should be configured.
- Different pieces are set up so that people will use them (and put their information in the right place).

Folder	Exchange/O365	Exception*
Inbox, Sent Drafts, Journal, Junk, Outbox, Spam, Synch	90 Days	Legal Hold
Retention Tags	Working Docs - 2 Years Records - 10 years	Legal Hold
Calendar	13 Months	Legal Hold
Contacts, Notes, To Dos	Indefinite	Legal Hold
Deleted	7 Days	Legal Hold

* A **legal hold** will suspend the deletion of potentially relevant mailbox items from Exchange while the hold is in effect.



EMAIL FILE PLAN AND ARCHIVE POLICY - DECISION MATRIX
Exchange

ID	Topic	Sub Topic	Detail	Question	Recommendation	Additional Considerations	Status	Decision	Decision Implementation Timeframe	Made By:	Comments
1	Exchange	Retention	Managed Folders	What Personal Regention tags will be utilized for email retention?	Working Documents (3 years) Extended Retention (7 years) Permanent (99 years)		Core Team Recommendation				
2	Exchange	Retention	Retentoin Policies	Which employees will not receive personal retetion tags?	Contractors & Temps		Core Team Recommendation				
3	Exchange	Retention	Retentoin Policies	Which employees will receive Working Docs (3yrs) Retention Tag?	Every employee except Contractors & Temps		Core Team Recommendation				
4	Exchange	Retention	Retention Policies	Which employees will receive the 7 Year Extended Retention Tag?	Constuction, Treasurey, Tax		Core Team Recommendation				
5	Exchange	Retention	Retention Policies	Which employees will receive the 99 Year Extended Retention Tag?	Legal & HR		Core Team Recommendation				
6	Exchange	Settings	Personal Archive Mailbox	Should Personal Archives Mailbox be enabled in Exchange 2010?	No		Core Team Recommendation				
7	Exchange	Retention	Mailbox Quota	Should there be quota	Yes		Core Team				

Legend | File Plan Decisions | Exchange | Archive | Implementation Plan | Training | Policy | Audit & Monitoring | PST

This requires the establishment of a category hierarchy through which retention rules can be applied. This hierarchy needs to be developed so that it can be applied to all data, including data in the cloud, social media, local repositories (structured and unstructured), and email.

Looking at email in particular, an email retention policy and file plan should be created that will classify and manage email within an approved repository (for example, Exchange) and an archive. The email file plan should define the rules and organizational structures for maintaining legal and business records in email servers and archiving systems. They can also be used to configure the settings of an archiving application. Email retention strategies can be based on role, function, business unit, position, or a combination of all of these. Effective file plans sort out this complexity, providing intuitive yet compliant retention strategies. The email organization structure should be such that it conforms to the corporate records management program and RRS.

Data files in other repositories, such as SharePoint or unstructured environments, should also be configured in a similar manner, applying standard, consistent taxonomies and file plans to properly reflect established retention policies.

K. Behavior Change Management, Communications and Training

The organization now has the policies and processes, roadmap, tools, and technology in place, so they think they are done. They are not. The organization now needs to get the employees on board and properly using the new tools that have been put in place.

Change management, including communications and training related to this initiative, is a critical element to drive user compliance. These efforts help to ensure effective implementation of the new structures and processes by affected employees and to demonstrate compliance with legal and regulatory requirements. Designed to drive users toward a target behavior set and to measure progress in achieving compliance, these activities are also beneficial for providing formal, consistent communications to employees and executive sponsors during implementation. With the proper metrics, tangible results can be illustrated, such as the impact on retention behavior, document retrieval and management time, reductions in data/email stores, increased levels of transparency, and increased effectiveness in responding to records requests.

An effective IG program requires more than documented policies and effective technology solutions. User behavior must actually change in order for the company to be compliant with policy and regulatory requirements. It is crucial that initial and periodic employee training and education and ultimate compliance be reinforced and enhanced on an ongoing basis.

This process involves understanding current employee practices (which was uncovered during the assessment) and developing and implementing a change management process that meets program goals and/or correctly utilizes new technology solutions. This will result in getting the organization to the desired future state. Change management is a formal activity – a discipline that can be mandated, and one that needs to be followed.

Category	Audiences	Definition
Executives	**Executive Sponsor**	John Smith – Program "Champion"
	Executives	Executive Committee
	Core Leaders	Senior Leadership, Regulatory Leadership Team, General Managers
Managers	**Managers**	Departmental/Functional Managers
	Records Coordinators	Designated representative of RIM program for specific functional areas
Employees	**All XYZ Employees**	

Employees need to understand what the policies are and they need to be using the right processes. They are now aware of their responsibilities and what the consequences are for non-compliance. Putting together an effective change management program involves working with a communications and training group to understand what kind of communication plans have been successful in the past in the organization and understanding what kind of platforms are available for training. Does the organization

have classrooms that can be utilized? Should the organization plan on using webinars, computer-based training or other on-line trainings? Putting together what are the particular audiences that need to be addressed, what platforms are available to deliver the training to the right audience, and looking at the messaging that needs to be developed are key considerations to ensuring a successful change.

VEHICLE OPTIONS	DESCRIPTION	DELIVERY RESOURCE	AUDIENCE		
			Executives	Managers	Employees
Senior Leadership Playbook	John Smith provides regular information to Executive Committee and Senior Leadership, to build awareness and get feedback	John Smith	X		
Town Hall Play Books	High-level overview of RIM Program rollout key messages relating to: Awareness, Timelines, and Training to pass on to XYZ employees during regular Town Hall meetings	BU Leaders / Managers		X	X
Departmental Meetings	5-10 minute presentations at scheduled departmental meetings	BU Managers		X	X

Computer-Based Training	30-minute module on RIM principles, new Policy and Schedule	iLearn	X	X	X
Online Messaging	Deliver different types of messaging (awareness building, how-to's, reminders, etc.)	Intranet	X	X	X

A comprehensive training plan, a thorough understanding of what content needs to be delivered, who should receive what type of training, and an appropriate timeline are all needed. An organization does not want employees coming up with their own solutions, subverting the policies and procedures that were so carefully and painstakingly developed. In order to get compliance, employees must buy in to the changes.

To summarize the above, some of the key steps in getting employees to accept and use the changes include:

- Development of a communications and training plan.
- Creating communications and training content.
- Applying the RIM policy to email and other information repositories.
- Training employees.

By following the above steps, the desired state can be reached where data is only in designated repositories, there is appropriate use and access of information, awareness of responsibilities and consequences, and reduced risk of unintentional disclosure.

The benefits of an IG behavior change management program include:

- *Drives User Adoption* – Drives program adoption by business units and employees.
- *Communicates Resonate Messages* – Identifies key messages likely to resonate with employees.
- *Sells Program as a Win* – Messages program as a win for all employees, not a compliance burden.

- *Tests Consistency* – Ensures messages and trainings are effective for all groups across the organization.
- *Demonstrate Compliance* – Demonstrates compliance with requirements and company intent to follow policies.

L. Disposing Legacy Data

It can be costly to hold on to information that is obsolete, expired, and not needed for legal, regulatory, or business reasons. Now that an organization has taken care of its new data, it is time to go after the old, legacy data – both electronic and paper/physical. It is time to develop a defensible deletion plan of legacy email, electronic documents, backup tapes, and paper and physical records and information, thereby reducing storage costs and lowering the risk and expense of discovery.

An organization must determine what needs to be saved (meaning, it can identify what can be disposed). Policies can be developed that include both the business justification and process for deleting electronic documents, and establish consistent, repeatable, defensible processes that allow for the routine deletion of data not under a legal hold.

Putting defensible deletion into place means investing time and effort to:

- Measure total data volumes across all media types.
- Define retention policies that include the business justification and process for holding on to information.
- Create deletion objectives and measurements across all types of media, including email, files, and backup tapes.
- Training employees to "save smart" and monitor ongoing effectiveness.

Paper and other physical records need to be a part of the remediation plan as well. A plan must be developed for the disposition of inactive, boxed paper records and other physical media. This includes the identification of owners, locations, and gaps in current processes, as well as recommendations for the use of internal resources versus third-party vendors. A standard operating procedure (SOP) can be developed to guide records managers and other responsible employees in the execution of records scoping, sampling, and classification (e.g., what to destroy, keep, and review).

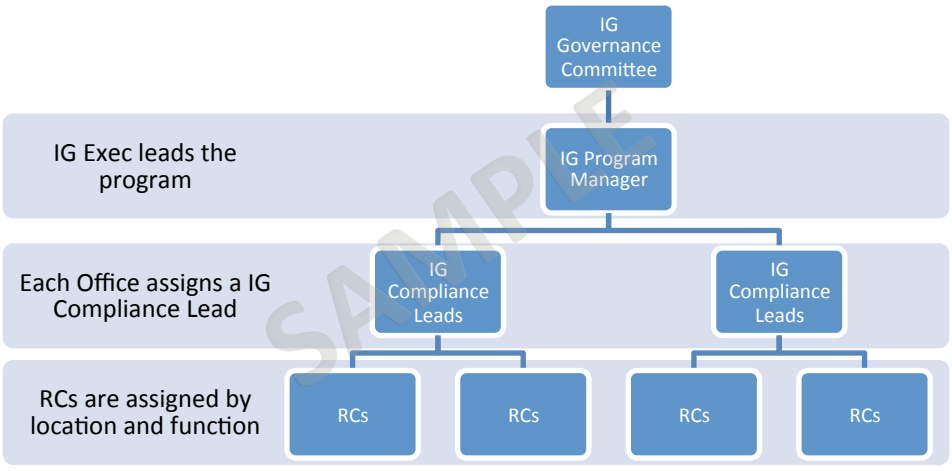
Since an organization has followed the above IG strategy plan, it now has retention policies and procedures, file plans and disposition rules based on proper classification for all of its information. Remediation of legacy data can begin. The strategy to conduct the remediation includes:

- Development of a defensible approach for indexing, classifying, and retaining or deleting legacy backup tapes.
- Classification of legacy tapes by disposition categories, including destruction targets.
- Optimization of backup tape procedures, aimed at producing smaller, more manageable sets of tapes by saving data with like retention periods on the same media.
- Identification of legacy tapes eligible for immediate deletion.
- Deletion procedures memorialized for ongoing use and deletion scoping and planning completed.
- Reduction of offsite storage costs, the risk of keeping documents too long, and the cost of review in legal matters.

Once the old, legacy data has been addressed, organizations should allow for an annual "information clean up" day on the IG roadmap, one that includes both electronic and paper (or other physical) information.

M. Information Governance Organization Development

An information governance management organization (IGMO) is essential to the proper execution of a comprehensive IG program. The IGMO should have the authority to enforce the records management policy and implement the RRS across all of the business units, provide oversight of the records management program, and provide assistance to employees so they understand their responsibilities.



An IG project is not a one-time project – it is a living project with ongoing capabilities within the organization. There are issues that are thought out throughout the project, such as:

- Identifying the right coordinators.
- Identifying the right stakeholders.
- Organizing a steering committee.
- Identifying who should be part of the steering committee, including executive level personnel.

The creation of (or update of an existing) a matrix structure of the strategic governing body (steering committee) will drive on-going IG activities and organizational compliance. The IGMO needs to bring together diverse professional viewpoints from various key business functions from across the organization. It also needs to ensure that there is good communication of requisite concepts, promote best practices for the management and control of the organization's information, establish cross-functional ownership, articulate goals and business benefits, and define ongoing roles and responsibilities.

The IGMO should oversee the creation of guidelines for IG and records managers as well as records coordinators, including their respective roles, responsibilities, and selection processes to ensure sufficient resources are devoted to participation and compliance efforts. Included in this should be the development and delivery of training content that is designed to inform all employees, not just those who are part of the records staff, of their key responsibilities and actions. Also included should be processes and procedures that are developed to be repeatable, consistent, and sustainable for control and management of records and all other information.

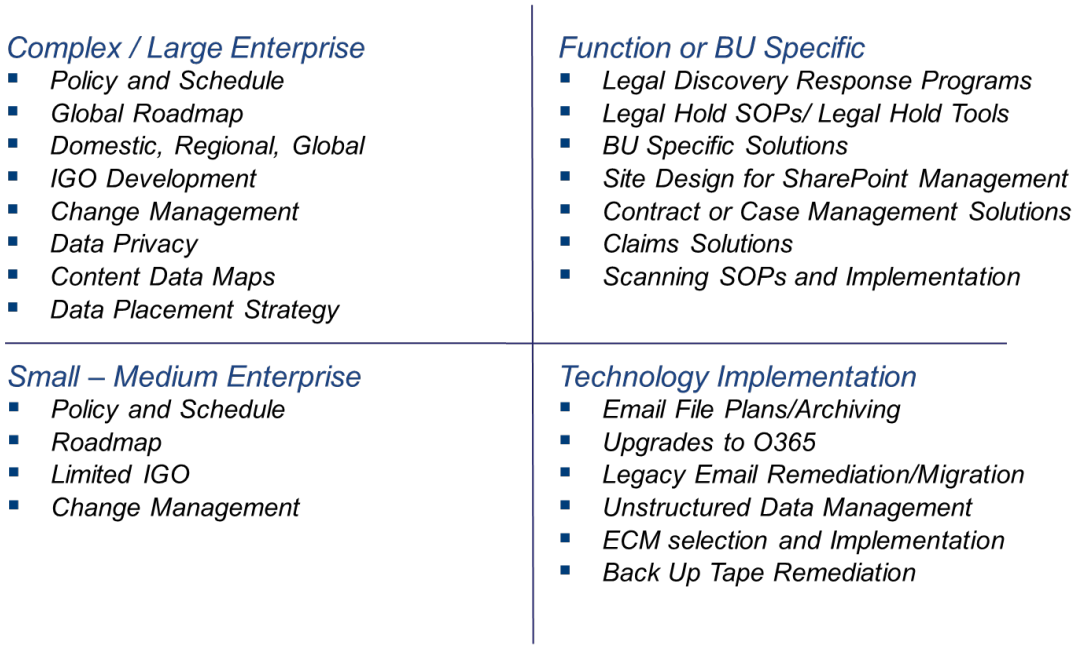
- *Establish Cross-Functional Ownership* – An organization must engage the representatives of business functions, such as information security, auditing, legal, compliance, and IT, to assist with the planning and execution of IG program initiatives.
- *Articulate Goals and Business Benefits* – Clear and specific business-related program objectives must be defined that ensure the support and commitment of stakeholders.
- *Define Ongoing Roles and Responsibilities* – An organization needs to establish work expectations and responsibilities for the IGMO participants, including identification of subject matter experts, the development of the criteria and process for selecting a records manager (RM) and coordinators (RC), communicating with and training RMs, RCs, and other employees with respect to their assignments, responsibilities and anticipated timelines, and mapping RCs to functional areas and regional locations.

The benefits of establishing and maintaining an IGMO include:

- *Defines Clear Ownership* – Defines cross-functional roles and responsibilities for IG across the organization.
- *Consensus* – Key stakeholders are aligned and in agreement with business units on roles and responsibilities.
- *Consistent and Complementary* – Custom developed to match business structure and environment.
- *Ongoing Management* – Proper structure is in place, designed to ensure ongoing program oversight and sustainability.

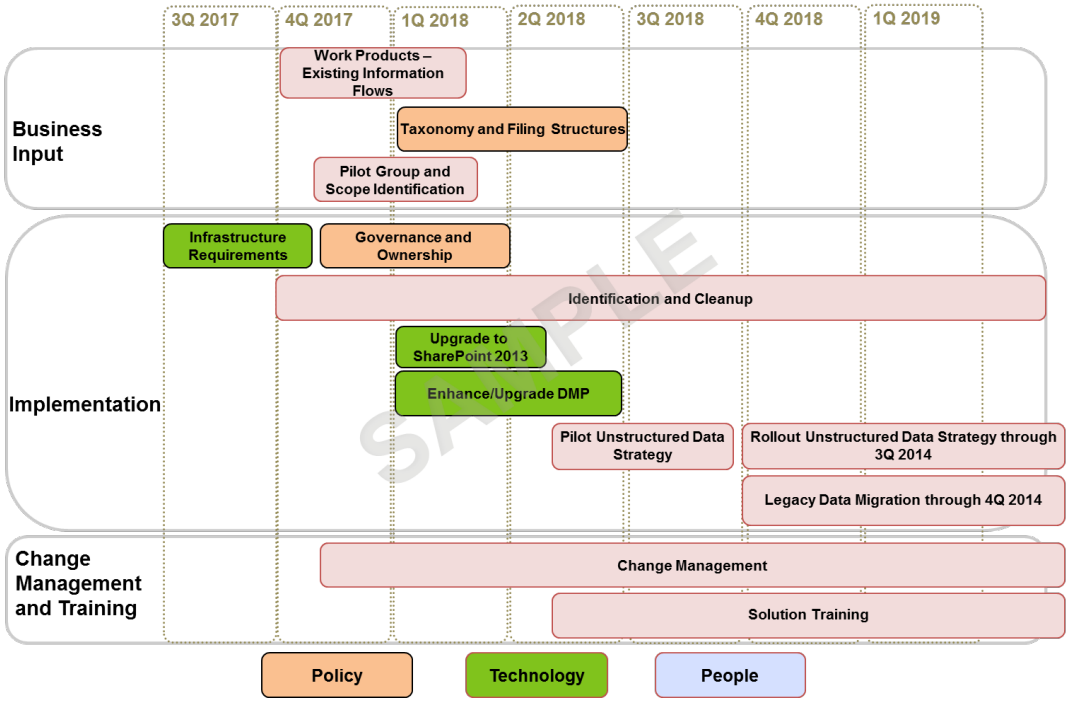
N. Sample Project Plans

Like the organizations they serve, Information Governance project plans vary tremendously. Some key elements of an IG project plan include:



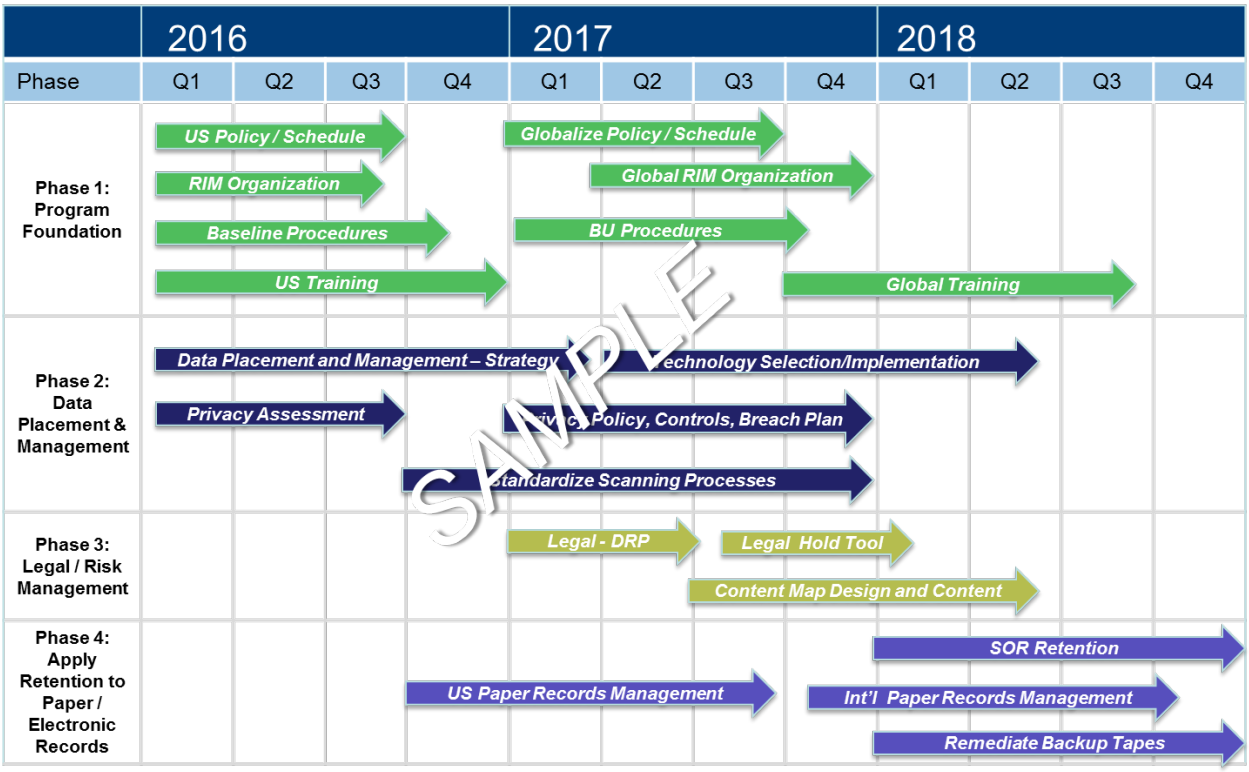
1. Simpler Project Plan

Here is an example of a simpler project plan running over seven quarters:



2. Project Plan for a Global Organization

Listed below is a more complex, multi-year project plan:



O. How to Avoid Getting Stuck

As discussed above, the biggest risk with any IG initiative is, quite frankly, getting stuck. Anticipating delays or roadblocks can be key to avoiding getting stuck.

What are the usual problems?	
Typical Problems	Solutions
Lose key Stakeholder	Recommendation: Identify and engage a cross-function group of Stakeholders. It is not enough just to have RIM, Legal, or Compliance or IT.
Budget issues	Recommendation: Define a realistic set of projects and cost estimates up front. Make sure to account for budget cycles in your planning process.
Competing initiatives	Recommendation: Projects such as Email, SharePoint, and Privacy/Security may already be in process. Look for opportunities to leverage work/projects that are already in the pipeline.
No one can make a decision	Recommendation: Clearly define roles and ownership at the beginning of the project. Core Team participants need to be engaged on a weekly basis.
Focusing too much on "technology solution"	Recommendation: Technology isn't the answer…it's only part of the solution. Set up the foundation first and make sure requirements are understood before moving to selecting technology solutions
Delays due to technology purchases	Recommendation: Make sure budget and approval cycles are known. Build in realistic timeframes not only for the purchasing process but also for configuration and testing

V. Defining Information Governance Metrics

Organizations face questions when launching an IG program: How can it be proven that what is being done is working? How is compliance demonstrated to regulators and courts? How is progress measured and reported to key stakeholders? To be able to answer these and other questions, organizations should incorporate metrics into their IG programs.

A. Tracking Program Success and Avoiding Failure

Compliance programs, unfortunately, often face a high failure rate. This is especially true for IG projects. According to Gartner, 50 percent of content management projects are rolled back out of production, a rate higher than other IT programs. This failure rate tends to breed skepticism by executive management. Even after business cases for IG-related projects are approved and slated to move forward, 75 percent of executives still believe these types of programs are not going to be successful.[3]

Regulators and courts often scrutinized these programs. Sometimes, in-house counsel believes creating a detailed policy will satisfy regulatory requirements. Regulators want to not only see a company's policy, but also see that the company is able to demonstrate compliance with the policy. The U.S. Federal Sentencing Guidelines, for example, require organizations to monitor and audit the effectiveness of compliance programs. An information governance program is no exception.

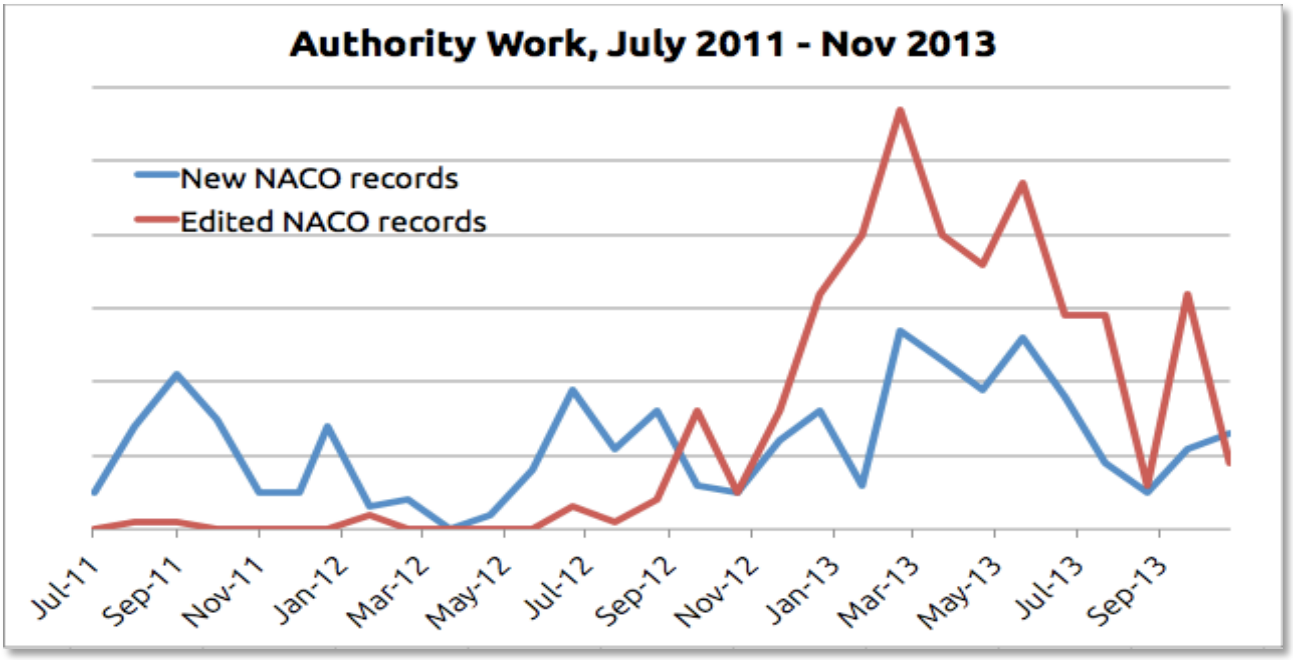
Likewise, in litigation, it is common for opponents to seek out and examine an organization's policies, looking for evidence on whether the policies were followed and seizing upon any indication, or even appearance, that an organization did not follow its policy. Organizations that can demonstrate compliance with their policies will be more defensible. For these reasons, creating a credible, compliant, and defensible IG program requires some level of objective demonstration that policies and processes are being followed.

B. What Are Metrics?

Increasingly, organizations are measuring their IG program through the use of metrics (a type of objective measurement). Metrics can be defined and measured in a variety of ways:

- *Absolute Value* – For example, a specific number on how many records exist or the number of people trained in records management.
- *Percentage towards a Target or Goal* – For example, the percentage of privacy information secured.

- *Comparison to Another Metrics* – Comparing two different things, such as amount of ROT vs. average eDiscovery cost for a small matter.
- *Relative Change* – Were improvements realized from last quarter to this quarter?

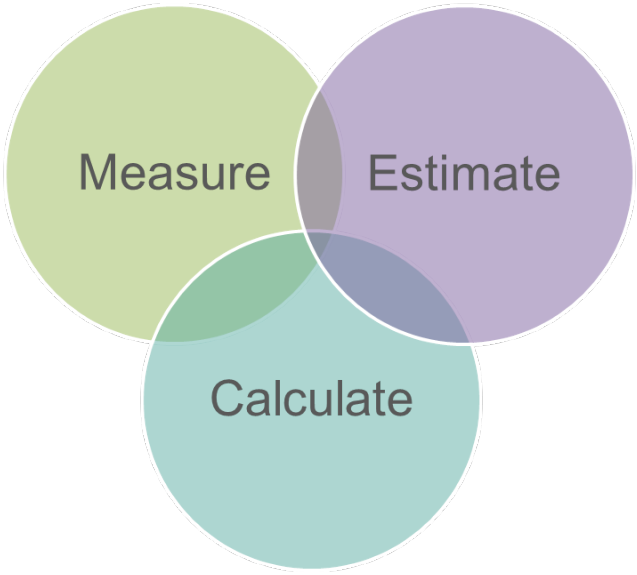


Most organizations use metrics to measure current state and then track progress over time. Metrics answer a number of questions:

- Did the efforts result in improvements?
- What areas experienced the biggest change for the efforts?
- What remains unchanged despite the efforts?

Metrics also serve as an objective key performance indicator (KPI) for senior management, allowing them to see tangible results for the resources invested. Often, metrics are used to demonstrate to regulators and courts that policies are being followed. Additionally, many metrics can directly feed into and support a formal ROI model.

C. Can IG Programs Be Measured?



Information Governance programs often encompass, literally, millions of records, documents, and data objects from potentially thousands of systems and locations. Do metrics attempt to count everything? Simply stated, no. Effective IG programs use three methods for populating metrics:

- *Measure* – A measured metric can be counted and computed. For example, one metric may be the percentage of divisions with up-to-date records retention schedules (RRS), as the number of divisions may be known, as well as which have RRSs. A metric could easily measure this. If nine out of 64 divisions have up-to-date RRSs, then 9/64 (or 14 percent) of divisions are up-to-date.

  It is important to measure something meaningful. For example, if two of the largest divisions (comprising 40 percent of the company) do not have updated RRSs, measurements will be less meaningful. Perhaps, a more appropriate and meaningful metric would be the percentage of employees working under an updated RRS.

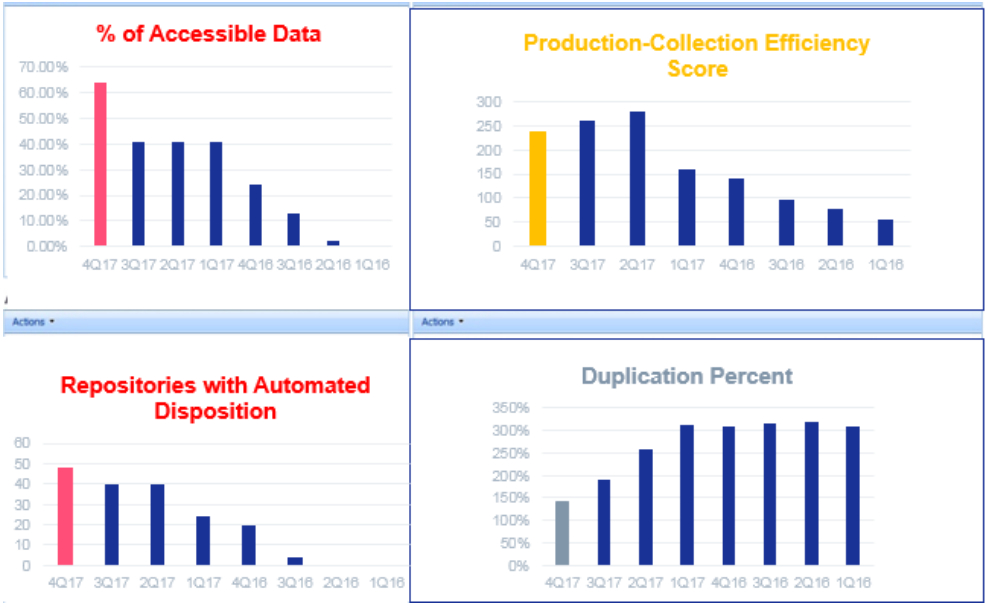
Note that initially, when documents and data reside in the "wild" (i.e., in unmanaged environments), it is difficult to provide these hard, measured counts. Often, organizations will use estimation and calculation techniques. As documents and data, over time, move to more controlled environments (such as archiving systems or records management systems), it is easier to provide a measured metric.

- *Estimate* – Not everything, however, can be directly counted. In some cases, metrics need to be estimated. The number of records properly managed or the amount of privacy information properly secured can be estimated by taking samples across a variety of systems. Estimates are not as accurate, of course, as direct measurements, yet less-precise metrics (derived from estimates) can still provide meaningful information and comparison.

- *Calculate* – The third method is through calculation. A calculation creates a relative score. For example, the ratio of records stored on-site vs. offsite at a storage vendor can be easily calculated.

Internal Box Count / External Box Count	=	2,201,221 / 3,535,184	=	Score 0.62

Good metrics can be thought of as a dashboard from program success. They should be understandable by key stakeholders and meaningful to the business. Likewise, they can continue to feed into ROI models, becoming more valuable. These can and should be updated over time to track progress, as well as recognize program weaknesses that need to be addressed.



The task of updating metrics also can become easier over time, especially as content "in the wild" migrates to content management and archiving systems. Many of these systems have the capability of providing direct measurements. Overtime, companies move away from estimations to measurements.

D. Sample Metrics and Examples

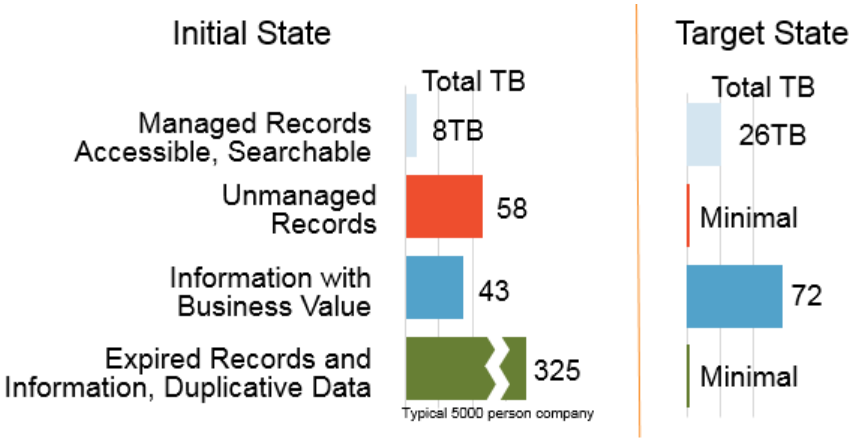
Metrics can summarize IG program effectiveness in the following areas:

- *Legal & Compliance* – What percentage of records across the enterprise are appropriately managed?

- *Privacy & Security* – What percentage of sensitive information is controlled appropriately?
- *Defensible Disposition* – How many documents and records are expired, unneeded, or have low business value?
- *Optimized Discovery* – What is the cost of discovery for small, medium, and large matters?
- *Productivity & Collaboration* – How much time do employees spend saving and searching for information?

Each of the above categories may have either a few or many metrics. It is important, however, that all this information can be "rolled up" into a few simple and easy to understand measurements to track program progress.

1. Legal and Compliance Metrics

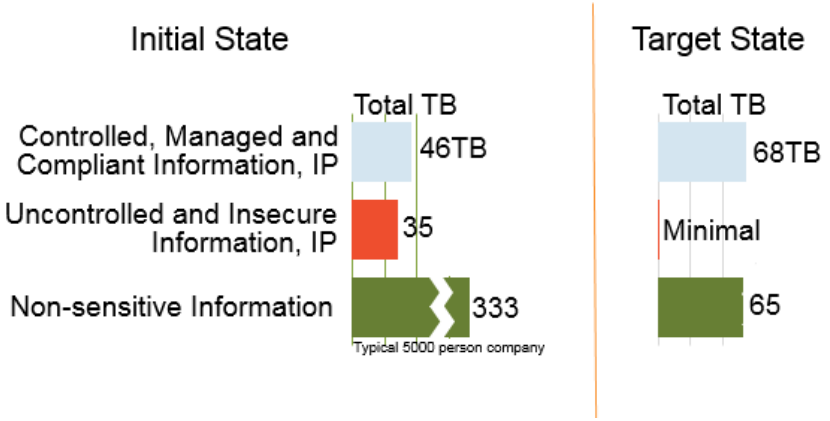


A sample of Legal/Regulatory records management metrics includes:

- *Percentage of Records Managed Appropriately* – The percentage of records managed in accordance with generally accepted principals.
- *Percentage of Structured Records Managed Appropriately* – The percentage of records being managed in accordance with approved RM policies with a defensible disposition.
- *Retrieval Time* – Average time to search for and retrieve a given type of record (useful when faced with regulatory retrieval requirements).
- *Record Classification* – Percentage of records that have tagging or metadata associated with them that can be utilized for deletion at the expiration of their retention period.

2. Privacy & Security Metrics

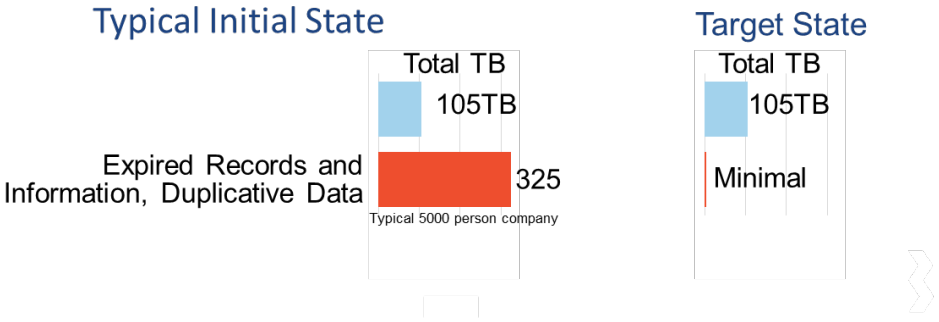
Often, organizations believe their privacy, IP, corporate confidential, and other sensitive information is managed appropriately because it resides in secure repositories. Unfortunately, this is often not the case. Employees will often take extracts of this information and store it in files on, for example, lightly-secured file shares. The result is that while much of the sensitive information resides in secured repositories, there may be large quantities of this information not appropriately managed. Good metrics recognize and track this, helping drive better security and management over time.



- *Uncontrolled Sensitive Information* – Percentage of privacy or other sensitive information that is not properly managed.

Again, good metrics should be customized to be meaningful to the organization and, at the same time, be clear and intuitive.

3. Defensible Disposition Metrics

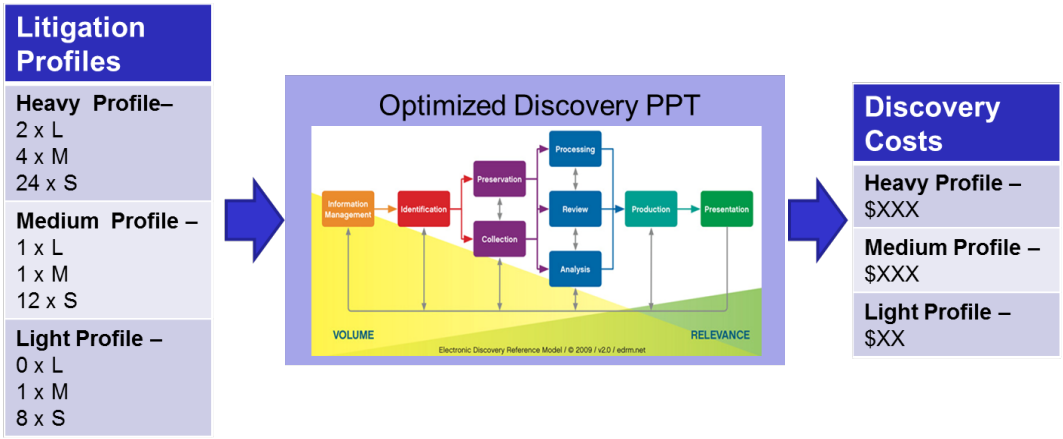


- *Number of Terabytes (TB) of Unstructured ROT* – Total volume of redundant, old and trivial electronic files.
- *Percentage of Unstructured ROT* – Percentage of a file shares or other repositories that contain ROT.

- *Percentage of paper ROT* – Percentage of paper or physical records containing ROT.

Note that ROT data and documents may reside not only on primary storage repositories (such as file shares), but also in many less accessible areas (such as backup tapes and offsite paper record storage). These areas often go unnoticed until they resurface as a result of a discovery need or potential breach. Good metrics look at all repositories and document stores.

4. Litigation Readiness and eDiscovery Metrics



Litigation is variable, which makes developing metrics for litigation readiness and eDiscovery difficult. Next year's litigation profile may be higher or lower than this year's profile. How do in-house counsel measure progress on something so variable? If costs go down, is that because there was less litigation or because IG made the processes more efficient? Litigation readiness metrics can help answer these questions.

Many organizations are developing matter-specific use cases: for example, small matters involving employee disputes; or larger matters involving discovery around a mid-size contract dispute; or, large matters involving large class action litigations. While it is not known how many (if any) of these types of claims a company will face in a year, what can be measured are the discovery efforts, data, and costs associated with each.

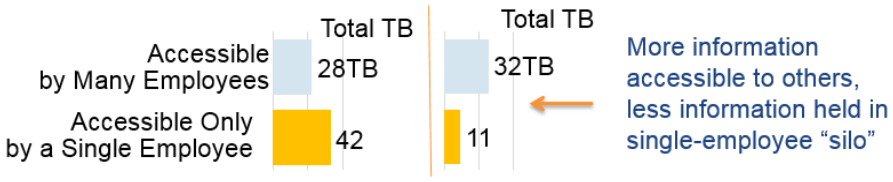
For example, today, a company may have to identify and review 200 GB of data for an employee dispute at a cost of $51,000. In the future, with much of the ROT data deleted, and the remaining information made much more accessible and discoverable, the same type of dispute may now only involve 80 GB of data at a cost of $12,000 to review. Not every case is the same, yet enough of these "rough" data points can be measured and enable litigation readiness and IG effectiveness around litigation to be measured.

Metrics in this category could include:

- *Production/Collected Ratio* – A calculated metric that typically is defined to include costs and volumes related to the actual law firm costs. This ratio is typically used to determine the efficiency of discovery and initial review by third party vendors. The efficiency is largely determined by the amount of ROT and inaccessible data.
- *Number of Days to Initially Provide Data for a Matter* -- The average number of days from the time a hold is identified to when the first data is provided to the regulator or opposing counsel.

Admittedly, developing metrics for litigation readiness is more complex. Nevertheless, IG improvements driving better eDiscovery processes can have the biggest impact on organizations.

5. Employee Productivity and Collaboration Metrics



Ongoing accumulation of data and documents adversely affect employees' productivity. They may spend many unnecessary hours each week searching emails, files, versions, and other information. Good IG programs can make valuable business information more readily available to employees and allow them to better collaborate with each other. All of this can be tracked.

Sample metrics can include:

- *Records Accessible* – Percentage of records accessible by a single individual or more than one employee.
- *Hours Spent Searching* – Average hours spent searching each week for email, files, and other electronic information.

VI. Record Retention Policies and Schedules

Many records management, privacy, discovery, and other information governance-related policies were created in a paper-centric or siloed world and did not include electronic documents. They were developed around best practices that were in effect at a time when paper was the primary communication and recordkeeping medium. Paper-based documents are treated differently (people do not carry large quantities around with them) and have a different cost structure (storing and accessing paper is expensive). These policies, for example, do not reflect the "far flung" and multiple-copy nature of email. Also, many of these policies do not reflect the need to preserve information in the event of litigation, or are not clear about which documents should be retained and for how long.

Some of these older policies call for destruction of documents that the currently applicable statutes require preserving, or they specify retention periods that are too short. Equally important, they do not set clear guidelines for deleting older documents that are not subject to preservation under litigation and are no longer needed. These types of issues and lack of clarity can be (and is) exploited by opposing counsel as evidence of a lack of good-faith and reasonable preservation efforts.

The massive volume of electronically stored information (ESI) and newer legal and regulatory requirements for retention and privacy require updated policies. Many older policies may need to be updated to reflect a media-agnostic approach that does not, for example, classify email as a record type, but rather recognizes email as a medium that contains both records and non-records. Additionally, many organizations are updating their policies to synchronize the practices for securing records and privacy or confidential information.

In the view of litigators, perhaps worse than an outdated document retention policy – or even no policy – is a policy that is inconsistent or not followed. A typical example of this is a policy that calls for the immediate deletion of all expired documents, while some users still save or print documents. During litigation, when an opponent can show that the policy was not followed, this can be used as justification for significantly expanding the scope of discovery or to imply that the inconsistent implementation of the policy was due to the company hiding information. Such an interpretation may be false, but it can play well during litigation.

Beyond the legal implications, a current and well-communicated policy provides guidance to employees that can help them make appropriate decisions – whether those involve retaining records that the business needs, or destroying records that are no longer required.

A records management policy specifies the overall philosophy of records management across the entire organization. This document should be framed in terms of general goals and responsibilities so that it does not require frequent revisions. It serves as a strategy for records management rather than a tactical execution plan or compendium of implementing procedures. The approved policy should be widely available and easily accessible to all employees and departments and supported by other, more specific documents, such as the records retention schedule, the litigation-hold procedures, and the training materials for specific recordkeeping applications.

A. Practical and Impractical Uses for a Record Policy and Schedule

Good policies balance different business and legal needs with ease of execution and costs. Attributes of good records management policy include:

- *All Types of Electronic and Paper Documents Are Included* – Good policies cover all types of documents, including files, databases, and paper (or other physical format), e-mail, instant messages, and social media. Likewise, they are comprehensive across the enterprise, including all types of ESI, and all groups and functional areas.
- *Are Clear and Simple* – Good policies and their corresponding records retention schedules tend to be simpler and, hence, easier to execute, especially for ESI, and they can be followed consistently.
- *Records Classification and Tagging Can Be Automated to the Greatest Extent Possible* – The sheer magnitude of ESI requires automation. Where possible, the document retention and discovery should be automated. This starts with having an "automatable" policy. For electronic documents in particular, policies should favor simpler and fewer retention policies – such that document retention and expiration can be automated to the greatest extent possible.
- *Minimizes Manual Processes* – Good policies tend to minimize manual processes. Manual processes tend to be more expensive, and very difficult to ensure consistent compliance.
- *Are Legally Defensible* – Most records management policies and records retention schedules will be discovered during the course of litigation. The opposing party will be looking to see if the policy was comprehensive and if it was followed. They will be looking to exploit any gaps between what you said you were going to do and what was actually done.

B. "Big R" vs. "Little r" Records

Organizations are often reluctant to engage in deletion knowing that some of the records must be retained for a period of time to satisfy regulatory or legal requirements. These can be referred to as "Records" – with a capital "R." Another category is "records" – with a

lower-case "r" – information that has business value but for which there is no external mandate to keep. Everything else can be referred to as "transitory" information. Best practices dictate that RIM professionals take the lead in guiding the definition, identification, and classification of "big R," "little r," and "transitory" information with policies and procedures embodied in a records management program.

One common mistake organizations tend to make is that such programs are focused too narrowly, often solely, on the "big R" records. Other parts of the organization may see value in content beyond "big R." The policy update process is an opportunity to better harmonize management of both records and content that have business value. It is a chance to build a consensus with the business units on what should be saved and what should not be saved. A good cross-functional team can decide on priorities and resolve conflicts.

C. Four Strategies for Gathering RRS Information

Developing a records retention schedule involves data collection for the types, custodians, and usage of documents across the enterprise to then be classified as records. There are different methods of conducting this data collection:

- *Modifying Off-the-Shelf Records Retention Schedules* - Obtaining a template RRS either from a law firm or a purchased database is, perhaps, the easiest and fastest approach of creating an RSS. Slight modifications, utilizing naming conventions or other company-specific details, can then be made.

  The advantage to this approach is that it provides quick results and has little disruption on the rest of the business. In addition, some of these systems provide automatic citation updating services.

On the other hand, one disadvantage is that these "pre-defined" RRSs often describe the records that a company "should have" and not necessarily what they actually have, making these RRSs less accurate and less compliant. Perhaps equally important, this approach, while capturing the regulatory requirements for "Big "R" records, often skips the business value of "Little r" elements – both of which are needed to create both as an official and employee-driven policy. Although a quick approach at the beginning seems like a good approach, in reality, it makes it more difficult to properly manage information later on in the process. An RRS with categories that meet legal and organizational needs better enables the execution of an effective IG program.

- *Online Surveys* - Another approach is to leverage a baseline RRS and then validate it through online surveys. This method works especially well for geographically distributed organizations with a number of remote offices.

  The challenge with these types of surveys is that the quality of data tends to be poor. Many survey recipients either ignore the survey or answer the questions in a cursory manner. Response rates from employees who actually carefully read

through the survey and diligently answer the questions tends to be low (between 3 percent to 6 percent). Sending more surveys to more employees can generate more responses, but the overall quality of the data tends to be lower.

- *Interviews* - The most effective data collection is through a series of either one-on-one or small group interviews. These interviews should take less than an hour and target a small set of employees spanning a wide variety of functions. The data quality from these interviews tends to be very high, and they are good for understanding exactly what types of documents and records are being received and created. Perhaps most important, interviews let employees feel that they are part of the process and being "heard," increasing the likelihood that the policy will be followed.

  The biggest drawback with interviews is the time it takes to conduct the interviews, both by the interviewer and the people participating in them.

- *Hybrid Approaches* - Often the most successful approach is a combination of the above, including interviews of core functions supplemented by surveys for more remote areas. It is important to get good data on record creation across key areas and then use surveys to validate that information.

  In general, deciding the appropriate time and resources to invest collecting data for records retention schedules, in part, depends on the complexity of the organization. Additionally, it is important to focus on the level of completeness, compliance, and consensus on the final RRS. Increasingly, companies are recognizing that time invested in creating a good RRS pays off many fold when these RRSs need to be executed.

D. Key Elements of a Records Management Policy

The policy document typically begins by identifying the overall purpose and scope of records management. Policies should be just a few sentences long and must make clear why the organization needs a records management policy. It should also make clear the types of records to be covered. The policy must speak in strong terms regarding retention periods, security, privacy, and storage of records. It must spell out whether electronic data (such as e-mail, instant messages, and social media), as well as drafts and convenience copies, are to be considered business records. It should also specify the roles and responsibilities of the records management staff, legal department, other employees, and outside personnel that handle organizational records and include provisions for handling violations of the policy.

Although Legal or Records Management typically leads policy development, IT does have an important role. IT needs to educate the Legal group on what are the capabilities of technology and how these would impact proposed policies. Likewise, IT needs to analyze and then educate Legal on the medium and long-term cost implications of various policies. Finally, IT needs to be involved in the development of litigation hold processes to ensure

that they can be automated (where possible), executed quickly, and the results will be defensible. It is vital to have IT at the table as the policy is being created.

E. Developing a Records Retention Schedule

Typically referenced by the records management policy, or included as an appendix, the Records Retention Schedule (RRS) specifies the amount of time each record type should be retained. That is, the RRS defines the minimum required retention period for each record category, typically measured in elapsed years after the record becomes final or inactive. In some cases, the retention period may start with a future event, such as "life of the contract plus seven years."

The RRS should also include a reasonably detailed, comprehensive list of all record types within the scope of the records management policy. The RRS can be organized by business function, with a number of record categories specified for each. Using the legal department as an example, the RRS would typically include line items for business organization, board and shareholder meetings, company ownership and stock transactions, compliance, contracts and agreements, intellectual property, litigation agreements, pleadings, correspondence, and legal opinions.

In some cases, organizations may want to treat many records the same way for purposes of retention and destruction. These can be grouped together to reduce the number of items in the schedule.

1. Inventorying Record Types

A good first step towards building the RRS is to have each department inventory all of their records. This can, however, be a long, tedious process that may require excessive time and effort, and can often lead to too much detail or company-specific definitions. Starting with a template can both save time and serve as a guide for the right level of detail. The records for different organizations in the same industry are remarkably similar, and many support groups (e.g., Finance and HR) have records that can be defined universally across industries.

An inventory should utilize a method referred to as an Information Types Inventory (ITI), which forms the basis for the Records Retention Schedule (RRS). The ITI is a working list of record and information types, including departmental inputs on business requirements and document examples. Using a combination of review of existing documentation and in-person interview sessions with business functions across the enterprise, record and information types (discrete elements of information that need to be managed and protected) can be collected and confirmed. The ITI process includes identifying (or validating and

enhancing existing lists of) record types (including any existing RRS), identifying process outputs, and collecting record type examples during interview sessions.

The information gleaned during the ITI review can be used to specify recommended retention periods for each unique record class and, if appropriate, to reflect consolidation of the preliminary record types. The document should include a listing of record classes/high-level functional categories, grouped and organized for clarity and ease of use, covering business records retained by the organization. The RRS should also include selected examples for each record class to enhance end-user understanding of the meaning and scope of each class, as well as updates to associated procedures.

2. Applying Legal and Regulatory Requirements

There is some debate as to whether legal and regulatory citations should be included in the RRS. These citations not only define how long records must be maintained, they often describe how the records must be maintained (e.g., medium and location).

3. Advantages and Disadvantages of Legal Citations

The benefit of including citations in the RRS is that Legal often receives updates to citations (not just retention, but all changes to the law or regulation). If the retention requirements have changed, it is easy to identify impacted categories in the RRS, if the citations were included. The downside is that it can be a maintenance burden. For example, if the business decides to split a category into two separate categories, Legal must be engaged to re-align the citations. In an organization with frequent re-organizations, or that is experiencing mergers, acquisitions or divestitures, this burden could be high.

4. Understanding and Applying Business Value to a Retention Period

Typical decisions about the long-term retention of information are based on IT operational needs. Although holding on to content based on file system metadata – such as age or file size – makes it possible to capture and migrate content to lower-cost tiers of storage (such as a capacity-based approach) makes no allowance for the importance or confidentiality of such information.

A better approach is to supplement capacity-based retention rules with policies aligned with *business value*. For example, retention policies can be based on any or all of the following:

- External regulations or legal mandates that define what kinds of information to save and for how long.

- The requirement of departments (e.g., finance, manufacturing, and sales) or business units to save different information for varying lengths of time.
- Requirements to preserve certain historical information for operational continuity reasons.

The notion of value-based retention dovetails nicely with the concepts of records series, file plans, and legal holds that are essential to the discipline of "records and information management" (RIM). To make life easier, it is recommended that IT managers reach out to their RIM colleagues who have already dealt with issues about value-based retention policies.

5. Developing a Media Agnostic Schedule

While the choice of media must be considered, especially for longer retention records, the category definitions on the RRS should be media agnostic. That is, a contract should have the same retention requirements, regardless of whether it is signed on paper, scanned into an image repository, or emailed from outside counsel (assuming that each represents the official version of the contract). The organization must determine which format (media) represents the official version (and all others would then be considered non-records and should be managed as such).

6. RRS Organization Strategies

In the interest of efficiency and effectiveness – particularly for electronic records – it is wise to limit the number of different retention periods that employees and systems must manage. Many organizations are moving to a simplified system based on broad retention categories – sometimes called "big buckets" – and a limited number of retention periods (e.g., one year, five years, seven years, and ten years). Such a simplified scheme is much easier for employees to comprehend, especially when it must be implemented in a framework such as an e-mail inbox. It can also be easier for automated processes to implement.

One implication of this approach is that some of the record types that are grouped into larger buckets will be kept for longer than their legal minimum retention period. It is generally acceptable to retain information somewhat longer than a department wishes, but it is much less acceptable to trim the retention period shorter than desired (and should not be made shorter than mandated by rules and regulations). The increased level of policy compliance and record completeness may well compensate for the modest increases in storage cost and litigation review time.

An organization's mileage, however, may vary. It may be important to break out record types that represent very high volumes of paper records and expensive physical storage. Also, some record types with similar names may turn out to have very different requirements for recordkeeping behavior – in terms of retention, privacy protection, and contractual obligations, for example– and will need to be identified by separate RRS categories.

It is vital to pay particular attention to those records that must be retained for *at most* a certain amount of time. Health and other personal records that are kept for too long, for example, can cause the same jeopardy as other records that are not retained long enough. Deleting data in the electronic world of multiple copies and dispersed backups can prove tricky, so consider record retention from the very beginning. For example, if a record must be expunged, never store it on the same media as one that must be kept as this can cause a serious conflict.

F. Keeping an RRS Up to Date

The records retention schedule should be updated periodically to reflect changes in legal requirements and business operations. The review should, once again, include interviews with the business units to determine what may have changed. For example, there may be some records that are no longer appropriate to a particular department and other record types that need to be added. If the RRS includes citations, those must also be reviewed and updated as needed. Once a review has been completed, it should be reviewed and approved by in-house counsel and by outside counsel, as appropriate.

G. Sample RRS Formats

1. Record Classes by Business Function

Class Code	Record Class Name / Description	Official Retention
Accounting / Finance		
ACC1000	**Accounting / Financial Reports**	MAX3
	Reports that provide useful accounting and financial information to management, including aging and distribution reports. Does not include invoices, sales orders, cash receipts, or financial reporting for healthcare providers/entity expenditures. See ACC1020 for Accounting Transactions - Accounts Payable / Accounts Receivable. See ACC1280 for Financial Management Reporting - Healthcare Providers / Entity Expenditures.	
	Retention Event: Retain these records only as long as they are needed, up to a maximum of three years. These records may then be destroyed.	
ACC1020	**Accounting Transactions / Accounts Payable / Accounts Receivable**	6
	Records related to the receipt and payment of monies. Includes payment of financial obligations, petty cash, the management and distribution of commissions, employee relocation expenses, and the management of the employee expense reimbursement function. Also includes sales orders and cash receipts of payments received from customers. Includes customer invoices, monthly customer statements, collection receipts, and cash receipts. These records verify the purchase of goods and services, the accuracy of the invoice, and authorize payment. Includes check requests, vendor invoices, travel expenses, and cash disbursements.	
	Retention Event: The retention period begins the date the record is created.	

2. Record Classes Listing with Legal Citations

Accounting

Retention Code	Record Class Title	Record Class Description
ACC1000	Accounting Accounts Payable / Receivable	Records related to payment of financial obligations and receipt of revenues. Includes vouchers, vendor invoices and statements, requests for payment, check requests and authorizations, expense reports, reimbursement forms, intercompany billing, remittances, and other expenses. Also includes accounts receivable adjustments and records of invoices, revenue, and other income.

Retention Requirement: **7 Years**

Jurisdiction	Citation	Retention Period
California	2 CCR 18932.1(b)(2)(A)	1 Year
California	CCCP App. 3011	1 Year
California	CCRC 711(d)	1 Year
US Federal Government	29 CFR 1627.16	1 Year
US Federal Government	29 CFR 1910.146(e)(6)	1 Year
Utah	UCA 34-28-10	1 Year
Texas	34 TAC 3.173(d)(1)	1 Year Limitation of Action
Texas	34 TAC 3.432(c)	1 Year Limitation of Action
California	2 CCR 18932.1(a)	2 Years
California	CLC 1174	2 Years
California	CLC 1197.5(d)	2 Years
Ohio	ORCA 4109.11	2 Years
US Federal Government	29 CFR 516.6	2 Years
US Federal Government	29 CFR 575.8(i)	2 Years
US Federal Government	48 CFR 4.705-1(f),(g)	2 Years
US Federal Government	48 CFR 4.705-2(b),(c)	2 Years
US Federal Government	26 CFR 301.6501(a)-1	3 Year Limitation of Action
US Federal Government	26 USC 6501(a)(1)	3 Year Limitation of Action
California	8 CCR 11020(7)(C)	3 Years
California	8 CCR 110407.(A)(6)	3 Years
California	CBPC 140	3 Years
California	CLC 226(a)	3 Years
New York	12 NYCRR 472.2	3 Years
New York	NY CLS LAB 195	3 Years
New York	NY CLS TAX 1135(f),(g)	3 Years
New York	NY CLS TAX 658(g)(4)	3 Years

H. Special Considerations in Developing Global Policies

The citations should especially be considered when developing a global RRS. The retention periods often vary by country, and especially by continent. The pros and cons of including citations do not change with a global RRS, but the magnitude of the implications does. Another consideration is whether to separate the same category of records into distinct categories for shorter and longer retention countries, or to round up for the sake of simplicity, recognizing the impact of over retention. Each organization will have to weigh these advantages, and if the exceptions are few, there is another option: the category could be listed with the retention of the majority of countries, with outliers listed specifically as exceptions.

VII. Data Security Classification

Much of the information a company creates, receives, transmits, and stores contains sensitive information, which often has specific management requirements, including security and disposition. Increasingly, companies are incorporating management of sensitive information as part of their IG strategy. This section outlines the key concepts and recommended practices for creation of a Data Security Policy - a key component of managing sensitive information.

A. Sensitive Data Everywhere

Many organizations know they have sensitive information yet mistakenly believe that this information is stored in secure repositories. Even in tightly controlled environments, sensitive information often leaks from secure to unsecure areas. For instance, data may be taken from a secure repository and stored in an unsecured repository for convenience purposes, storage limitation reasons, or transitory storage reasons. Employees, contractors, and other authorized individuals often store confidential or sensitive data on corporate file shares, in email, or on portable devices (such as unencrypted laptops and USB flash drives). Once in this unsecure location, the data may simply be forgotten. Since unsecured repositories have an inherent lack of access control, it still represents a potential risk of a data breach or data leak. Couple the ever-increasing volumes of data that organizations are accumulating with the growing number of potentially unsecured places that data may reside, the risk of a breach or leak is much greater. Exacerbating the problem is the fact that employees are often unaware that they are prohibited from storing data in a particular location, or worse, the company may not have a policy prohibiting this type of behavior or any specific training on how to deal with a particular type of information.

A data breach is an incident where confidential or sensitive information has potentially been accessed, stolen, or used by unauthorized individuals, and can occur in a number of different ways. The most common type of data breach is from insiders – employees or former employees who have (or had) legitimate access to sensitive information. Disgruntled employees copy and disclose this information in either an unsecure or unauthorized manner. Another type of leak is inadvertent disclosure, where sensitive data is stored on a removable media (such as a USB "thumb drive") for access purposes and subsequently lost. The breach and subsequent harm occurs when the information is lost, even if there is no evidence that the lost data was accessed or used for nefarious purposes.

Although more discussed in the media (and less common) are threats from outsiders, where "black hat" attackers "hack" into the corporate network to steal data for financial gain. This is a huge problem because a hacker may have access to a wide range of data sources at a

variety of access levels. Another, newer type of leak, is a so called "WikiLeak," where large quantities of electronic documents are stolen and then sent or posted online for full public disclosure. The intent of Wikileaking is to damage or embarrass an organization with the hope that within the sheer quantity of documents released, some will contain hurtful information. Both governmental and private sector organizations have been victims of WikiLeaking campaigns. Many of these targeted attacks seek less protected information residing on lightly-protected repositories, such as file shares and desktops. Regardless of the mechanism or intent of the breach or leak, the consequences can be severe.

Rules and regulations have been recently developed or updated to help combat these issues. The strictest rules are coming from Europe under new Data Protection rules that require the protection of any information relating to an identifiable person. These rules require assessment, accountability, and stricter notification, and also come with strict sanctions.

A further complication is the "right to be forgotten," which is distinct from the right to privacy:

- *The Right to Privacy* - Protects information that is not publicly known.
- *The Right to be Forgotten* - Involves removing information that was publicly known at a certain time and not allowing third parties to access the information.

Though the legal protections for "right to be forgotten" are strongest in Europe, organizations in all countries must at least consider this as a required capability and design the ability to delete (or at least suppress the dissemination of) data that would be disclosed as a normal business practice.

Many other regions of the world have enacted "notice" laws, and in the U.S., most states have enacted some form of similar notice that requires the breached company to notify customers if they are involved in a data breach. There are also a number of industry-promulgated guidelines and government compliance regulations that mandate strict governance of sensitive or personal information to avoid data breaches. For example, the Payment Card Industry Data Security Standard (PCI DSS) directs who may handle and use sensitive personally identifiable information (PII), such as credit card and bank account information. In the healthcare arena, the Health Insurance Portability and Accountability Act (HIPAA) regulates who may see and use personal health information (PHI), such as name, Social Security number, date of birth, and health history information.

In today's business world, intellectual property (IP) is not only viewed as a legal asset but also increasingly as a financial asset. Organizations, such as those in knowledge-based industries (such as the high technology and biotech industries), spend most of their time researching and developing IP as building blocks of innovation. Intellectual property is

also one of the main assets looked at in performing due diligence for mergers, acquisitions, and divestitures. The valuation of one's IP assets, both from a financial standpoint and risk/liability assessment, weigh heavily on the minds of potential investors and purchasers.

Patents, a form of intellectual property, can also make up the bulk of a company's financial assets. Patents typically are developed over several years of research and development and the documents and records created in the development of the method, process, or technology can be quite extensive. Because of the exclusive rights derived from owning a patent, the financial value of patents has become more and more the subject of high stakes litigation.

One particular category of patent litigation that has been on the rise in recent years is litigation brought by patent holding companies or non-practicing entities. A patent holding company (pejoratively often referred to as a "patent troll") typically amasses a large amount of patents in a particular field, not to practice the claimed inventions, but to license the technology for others to practice. Patent holding companies also like to litigate those they believe are violating the patents in their portfolio. A typical practice of the patent holding company is to send a cease and desist letter to those in the target field or industry offering a license to practice the inventions covered in the patent(s). A recipient of a cease and desist letter is faced with one of two options: either fight the lawsuit (usually at significant expense) or pay the license fee (which is generally less than the total cost of litigation).

A patent holding company, typically, is looking to monetize their patents and obtain the most money with the least amount of expense. Organizations with limited ability to analyze their IP portfolios are likely to spend more during litigation and/or are more likely to settle these types of suits. Therefore, these unprepared organizations are a more likely target for the patent holding companies. Most patent holding companies engage outside counsel on a contingency basis and all costs are subtracted from the settlement or verdict amount. A quick win through settlement is often more attractive.

When it comes to discovery, many times, larger businesses are at an extreme disadvantage as they generally will have a much larger universe of responsive data to identify, collect, review, and produce than a patent holding company. Having a deep understanding of where an organization's patent related information is stored and how to retrieve it quickly and efficiently will enable the organization to be on the offensive side in the discovery process.

Another form of IP common in today's business world is a trade secret. Trade secrets are often an overlooked corporate asset because the very existence depends on secrecy and the fact that they are not registered with any government office or disclosed to the public. When taking inventory of IP assets, if the right identification and tracking procedures are

not in place, the full scope of a company's trade secrets may be overlooked. If trade secrets are the main source of IP for the organization, this could turn out to be a costly mistake.

As with any form of IP, organizations have the responsibility to protect their trade secrets. Trade secret owners have a duty to use "reasonable measures" to protect their secrecy. One of the main reasonable measures organizations employ is the use of confidentiality and nondisclosure provisions in employment contracts or other appropriate documents. Assuming that employees, contractors, and vendors are abiding by the provisions in their contract, there is the additional issue of understanding where the protected data is actually being stored.

Understanding what the data is, and where it is being stored, are the first steps in identifying, and subsequently protecting, valuable trade secrets. Unlike patents, trade secrets can exist indefinitely (e.g., Coca-Cola or Kentucky Fried Chicken recipes). In a world dominated by electronic communications across a growing variety of media, organizations face the biggest challenge with the third criteria: keeping information secret. Trade secrets can and have been leaked through emails, files, and other media, often inadvertently. In order to safeguard trade secrets today, organizations must demonstrate that they have an ongoing process for protecting this information.

In many organizations, private and sensitive information can be found just about everywhere. "Official" repositories that contain confidential data are often clearly identified, centrally managed, secured, and have proper disposition policies in place, yet breaches of privacy and confidentiality can arise from many sources. Some of those sources include:

- The "BYOD" trend and the storage of information on mobile devices.
- Moving information to insecure areas, such as file shares and email PST files, that lack appropriate access controls.
- Frequent and casual interactions among customers, partners, government agencies, and employees.
- The insecure handling and disposition of hard copy, removable media, retired PCs, laptops, systems, and servers.

For a 5,000-person organization, it is common to find that unsecured confidential information and intellectual property assets comprise as much as 10 percent of the total amount of stored information. Failure to properly manage this sensitive data can result in penalties, expense, and reputational damage.

B. Different Types of Data Need Classification and Controls

1. Organizations Have Different Types of Sensitive Information

An organization's large store of data typically contains a small amount of often accessed ("active") content, as well as a large portion of older, rarely-accessed ("inactive") content. Regardless of whether data is active or inactive, both types are likely to contain sensitive information. Depending on the industry, sensitive information can include legally protected personal information, such as credit card or other banking data, social security numbers, personal home addresses, or other PII that can distinguish or trace an individual's identity. It can also include PHI, such as medical history, insurance information, or other information regarding employee benefits or healthcare organizations. In addition to data about individuals, organizations also collect and store information that is sensitive for the organization as a whole – including confidential IP and other sensitive business information, such as financial results, business strategy documents, and executive communications.

2. Sensitive Information Exists in Structured, Unstructured and Semi-Structured Formats and Repositories

Data storage repositories contain data in a variety of content types and formats, including structured, unstructured, and semi-structured data, as well as messaging and backup systems. In many organizations, privacy and information security efforts tend to focus first on structured data applications and databases. However, highly-visible data breaches, such as Sony Pictures and Panama Papers disclosures, have demonstrated that significant harm can come to organizations that do not identify and control the sensitive information that exists in less-structured repositories of documents and messages, as well as in paper records and printed copies.

C. Create a Comprehensive Data Security Classification Policy

1. A Narrowly Focused Security Policy is Risky

As it assesses its privacy and security requirements and its current state, a company may discover that it has defined a privacy policy that focuses narrowly on one law or regulation, or represents a response to a single event in its industry or its own experience. Such a narrow policy may fail to identify and protect other types of sensitive documents or data.

2. Multiple, Inconsistent Policies Increase Risks and Costs

More commonly, an organization discovers that it has responded to different requirements and events by defining and publishing multiple privacy and security policies, along with inconsistent or confusing compliance guidelines.

For example, perhaps a privacy officer has defined data classification rules to control PII or PHI in specific databases or media types. Meanwhile, the information security team has issued guidelines for classifying and managing sensitive financial reports in file shares or email attachments, using different terms to describe the required data classifications and controls.

As a result, many employees are confused about the policy requirements, and behave inconsistently in their application of needed security measures. This situation increases the risk that sensitive data could be improperly disclosed or misused. It also tends to increase the costs of managing the data, ensuring compliance, and responding to changes in business requirements or technology capabilities.

3. Recommendation: Establish a Single Comprehensive Data Security Classification Policy

To avoid the risks and costs presented by multiple and inconsistent policies, an organization should establish a single, comprehensive Data Security Classification policy – one that addresses all the applicable regulatory and business requirements and provides guidance for the management of all types of information, in all locations across the organization. The policy document should identify the policy objectives, define key terms and requirements, and outline roles and responsibilities. It should also incorporate or reference a simple baseline Data Classification Standard (DCS), along with other documents that provide more-detailed procedural guidance:

- *Data Classification Standard* - A document that defines levels of security classification for records and information, and for the repositories (systems and media) that contain them. The standard also specifies the set of data-security controls that apply to defined activities that occur over the life cycle of the data.
- *Data Security Classification Policy* - A document that provides corporate direction regarding information security, including the implementation of an overall Data Classification Standard and the associated privacy and security controls. It may also include policy direction regarding additional classifications and controls that are needed to meet industry-specific privacy rules, or to comply with laws and regulations in specific geographic locations.

4. Keep the Security Classifications Simple

To enhance understanding and compliance, the DCS should define a few simple, easy-to-understand category labels, such as Public, Internal Use, Confidential, and Highly Confidential. As discussed below, the DCS should provide multiple examples for each category – to clarify the meaning of the category and help employees apply the classification to a variety of content types.

5. Adjust the Policy to Fit the Company's Data

The DCS provides a global, baseline set security classification that applies to all – or nearly all – content types and repositories. The DCS also specifies the minimum set of controls that employees and automated processes must apply to the data in each security classification during information management activities (including identification, storage, retrieval, duplication, transportation, archiving, and deletion).

The global DCS, however, may not address all of the data security requirements imposed by industry-specific regulations, local jurisdictions, contract provisions, or special situations. Examples of such requirements include:

- The SEC's prescription of tamper-proof media, to ensure data integrity when storing broker-dealer communications under Rule 17a-4.[4]
- Requirements to track and report any disclosures of PHI under the HIPAA Privacy Rule.[5]
- The HIPAA Breach Notification Rule.[6]
- The need to limit the retention period for personal information under EU data-protection directives.
- Case-specific document preservation and protection requirements, imposed during legal hold and discovery proceedings.

Rather than attempting to embed such requirements into the global DCS, organizations may recognize those requirements in the Data Security Classification Policy document – and then point to separate standards and procedures for implementation and compliance.

In some cases, a company may establish a separate repository that meets specific industry or contract requirements.

- Many securities firms, to ensure compliance with regulatory requirements and industry rules, have established special repositories for broker-dealer emails and messages.
- Many U.S. defense contractors keep government-owned documents and information in separate data repositories, protected with physical safeguards and

Data Loss Prevention (DLP) technology; or, in document management systems that meet the applicable requirements of DoD Standard 5015.2 (www.dtic.mil/whs/directives/corres/pdf/501502std.pdf).

Organizations, in most cases, can meet their industry-specific data security requirements by applying a global DCS to all information – and by identifying any known exceptions in the Data Security Classification Policy, along with pointers to additional standards and procedures.

- Specific privacy program documents, for example, may specify unique metadata tags – in addition to a standard Security Classification field – for electronic documents that contain PII or PHI.
- Employees and information systems must apply the security controls specified in the global Data Classification Standard and take the additional actions prescribed for documents data tagged as PII or PHI.
- This approach requires employees and systems to place the protected information in repositories that can support metadata tagging – and can also apply the required controls and reporting capabilities. An organization should consider such requirements when it develops its Data Placement Strategy.

6. Integrate the Data Classification Policy with Other Components of Information Governance

The design and implementation of the Data Classification Policy and the Data Classification Standard should be closely coordinated and linked with the other components of the overall IG program and roadmap, including:

- Records Retention Policy and Schedule.
- Data Placement Strategy.
- Repository-Specific File Plans.
- Information Systems Design and Implementation.
- Metrics, Reporting, Audit, and Verification.

For example, a small manufacturing firm might determine that the DCS labels can be integrated directly into its RRS – by inserting a "security code" column into the RRS – with only a slight increase in complexity. The RRS would assign similar record types to distinct Record Classes, despite identical retention requirements, to specify more-rigorous security controls for more-sensitive information.

In contrast, a diversified or highly-regulated firm might integrate the records retention and data security requirements only when defining file plans for specific repositories – or when defining an overall DPS to guide those specific implementations.

D. Create an Effective Data Classification Standard

1. Definition and Scope

A data classification standard (DCS) is a document that defines levels of security classification for records and information, and for the repositories (systems and media) that contain them. It provides a global, baseline set security classifications that apply to a wide range of content types and repositories.

The standard also specifies the minimum set of data-security controls that apply to data in each classification during activities that occur over the life cycle of the data, including identification, storage, retrieval, duplication, transportation, archiving, and deletion.

The DCS provides guidance for employees who perform these data management activities and system architects and administrators who implement specific controls and capabilities in the company's information systems and data repositories.

Thus, the DCS functions as a guide to managing systems and individual documents, to achieve compliance with information security and privacy policies – as required by laws and regulations, contract obligations, and internal business needs for protection of proprietary information.

The final standard typically reflects the adoption of an information security framework that is appropriate to the company's business activities – as illustrated in the following sections, with examples from different industries.

Additionally, a DCS is a key component of any IG initiative. When implemented correctly, the DCS helps to ensure application of appropriate security classifications and controls for each document and content type.

2. Consider Adopting or Developing a Security Framework

Regulatory authorities and industry organizations have developed and published a number of information security frameworks - a published document, or set of documents, that outlines an approach to data classification and security controls for different types of content.

An organization should certainly comply with any mandatory security frameworks and regulations that apply its specific industry or business activities. Furthermore, organizations should consider leveraging available frameworks as sources of overall guidelines -- and of specific language where appropriate.

The first step is to choose (or develop) a framework that organizes (or specifies) the needed security controls.

A few examples to consider, in consultation with the firm's information security staff and other stakeholders, follow.

3. Federal Information Processing Standards (FIPS)

The U.S. National Institute of Standards and Technology (NIST) publishes a number of documents that define information security requirements for Federal agencies (http://csrc.nist.gov/publications/PubsSPs.html).

Other organizations have also adopted these standards, especially educational institutions, state and local governments, and manufacturing firms that provide products under government contracts. The NIST publications provide a general-purpose set of specifications that any organization could use when developing its own framework:

- FIPS Publication199 - Standards for Security Categorization of Federal Information and Information Systems.
- FIPS 200 – Minimum Security Requirements for Information and Information Systems.
- NIST SP800-53 – Recommended Security Controls for Federal Information Systems and Organizations.

4. HIPAA Privacy and Security Rules (45 CFR Part 164)

The U.S. Department of Health and Human Services (HHS) has published detailed requirements for the protection of personal health information across all media types, the HIPAA Privacy Rule (http://www.hhs.gov/hipaa/for-professionals/privacy).

HHS has also developed more specific guidelines for protecting such information when it is created, stored, or transmitted in electronic form, published as the HIPAA Security Rule (http://www.hhs.gov/hipaa/for-professionals/security).

5. International Organization for Standardization (ISO) - Global standards

The ISO has published a number of relevant standards and framework documents, including the following (http://www.27000.org/index.htm):

- ISO – 27001 – Implementing an Information Security Management System.
- ISO – 27002 – Information technology – Security techniques – Code of practice for information security management.

Many large manufacturing firms, and other organizations with worldwide business operations, have utilized the ISO documents when developing or updating their information security frameworks.

Note that these ISO documents are not free, yet they do provide very detailed information. Organizations embarking on serious information governance and security initiatives should seriously consider acquiring these documents.

6. Use the Framework(s) as a Starting Point

An externally developed framework cannot fully specify all the relevant requirements in a way that fits a specific company's situation. A good framework, however, does provide useful input for construction of a Data Classification Standard in several ways:

- Identifies the three major goals of data security. For example, the FIPS 199 framework provides the following definitions, citing 44 U.S.C. 3542:
  - *Confidentiality* - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  - *Integrity* - Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.
  - *Availability* - Ensuring timely and reliable access to and use of information.
- Provides a method for assessing different levels of risk, and for considering the potential impacts of a security breach or a control failure on each of the three security goals.
- Provides charts or matrices that help an Information Security team to decide what types of controls should be applied to each type of content, repository, and data-management activity.
- Designates particular components or controls as required (mandatory) or recommended -- based on the types of information, the access requirements, the level of risk, and the potential impact of a security breach or control failure.
- Recognizes that the implementation of rigorous security controls must be appropriate for the level of risk and the potential impacts, and must be reasonable in terms of the organization's size and resources.
- Recognizes that information security implementation and improvement is an ongoing process that can be prioritized and implemented over time.

7. Select Meaningful Names for the Security Classifications

Choose a set of data security classification names that are meaningful in terms of the kinds of information the company keeps and the way employees work. To enhance understanding and compliance, the DCS should define a few simple and easy-to-understand category labels.

Like the RRS, the DCS document should provide multiple examples for each category (to clarify the meaning of the category and help employees apply the classification to a variety of content types).

The DCS should define and explain at least three classification names, but no more than five. The following examples, from organizations with different industries and business activities, may be useful as a starting point for discussion of appropriate security classification names. In each case, the classification at the top of the list represents the most sensitive information, and the DCS specifies the largest number of rigorous and mandatory controls for the top category:

Data Classification Standard Examples	
Simple Corporate Example (three levels)	Typical Corporate Example (four levels)
Confidential	Restricted

Internal Use Only Public	Proprietary Internal Public
Intellectual Property Company Example Extremely Sensitive Highly Sensitive Sensitive Normal	Government Agency Example Limited Official Use Controlled Limited Official Use Official Use

Note that the Government Agency example does not reflect the proposed naming conventions that the National Archives and Records Administration (NARA) (www.nara.gov) has proposed for "Controlled Unclassified Information" (CUI), but the listed examples are likely to be more meaningful for a general audience.

In each case, the classification at the bottom of the list represents the least sensitive information. The DCS will specify the smallest number of rigorous and mandatory controls for this bottom category.

When, from a security perspective, the information is classified as "Public," the standard may state that no security controls are required for any activities that affect the documents or data. Alternatively, the standard may require certain minimal controls to ensure document integrity and suitability for business use.

8. Identify the Controlled Activities

The DCS will specify security controls for identified activities that could potentially affect the confidentiality, integrity, or availability of the documents or data.

It is helpful to collect a list of terms, as they are commonly used within the organization to describe such activities. The next step is to group those terms, based on similarities, activity, or result, into activity types. There is no universally accepted list of activity types, though each of the example frameworks does provide a number of possible choices.

For example, the resulting list of activity types might include the following:

- Information Handling/Retrieval/Output.
- Information Sharing.
- Shipping/Transportation.
- Data Storage.
- Disposal/Destruction.
- Security Labeling.

To illustrate and clarify these activity types, the DCS can include a table that shows common examples for each activity type:

Retrieval / Output	Sharing	Shipping / Transport	Storage	Disposal / Destruction	Security Labeling
Access Control	Internal	Email	Physical (Paper)	Physical Media	Physical Media
Authentication	Third Party	Electronic Transmission	Datacenter	Electronic Media	Electronic Media
Auditing Levels	Via Voice	Mail/Courier	Removable Media		
Printing	Requests for Information	Transporting Domestic	3rd Party (Cloud)		
Copying		Transporting International	Backups		

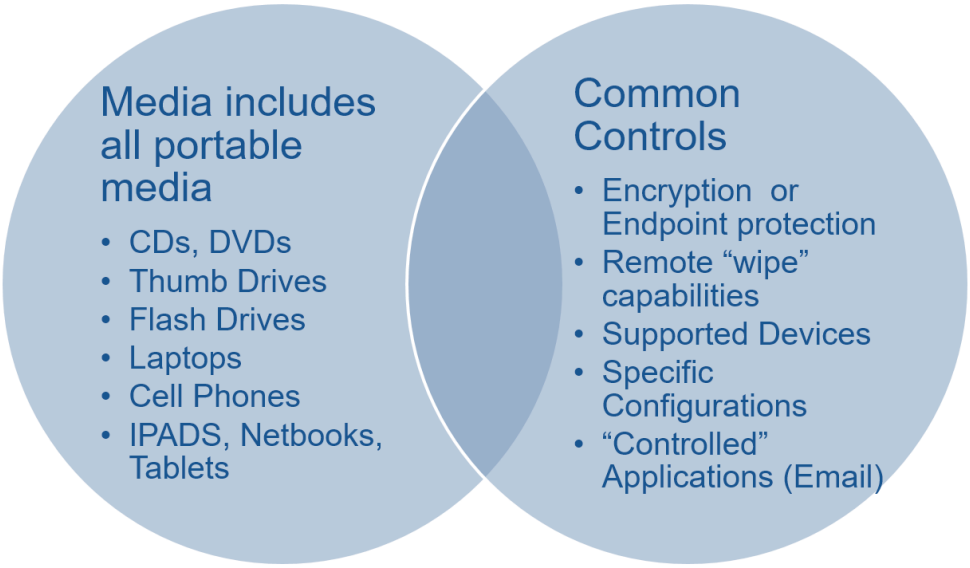
9. Identify the Security Controls

The DCS must specify appropriate security controls for documents and data in different security classifications. The applicable controls will depend on the activity type, and the capabilities of the information system or the characteristics of the data storage medium or device.

Data security frameworks provide useful lists of administrative, physical, and technical controls in functional terms (such as access control, authentication, data encryption, and media erasure or destruction).

A good framework, however, such as the HIPAA Security Rule, avoids specifying the exact technologies that must be used when implementing a particular control capability. To identify further the available controls, an organization's information security team can

provide a complementary list that reflects the actual capabilities and limitations of current and planned information systems. For example, the following figure illustrates the types of controls that might be applicable to the "Data Storage" activity when the data is stored on removable media.



10. Specify the Controls for Each Data Classification and Activity

The DCS should include tables that show the types of controls that apply to each activity type, for each security classification, on a required or recommended basis.

These tables can be quite detailed and are developed for use in a specific enterprise as the final step in creation of the company-specific standard.

E. Implement the Required Security Controls

Implementation of the DCS should be integrated into the overall IG roadmap, including the following key steps.

- Identify which systems contain which classes of information through business outreach and/or information classification tools (scan the content), and prepare a system map.
- Assess the current control capabilities in each system or media type, as illustrated below.
- Determine whether it is best to keep information in existing systems or to restrict/move more-controlled classes of information to designated repositories that can apply the required controls.

- Create a gap analysis of current vs. needed controls.
- Prioritize the controls into the IG roadmap.
- Implement the controls.
- Monitor the results.

Returning to the example of portable media on which employees could be receiving or storing sensitive information, the following figure illustrates an assessment of current control capabilities for a particular enterprise.

Common Controls	Level %	Description / Comments	Applicable Policy Section
For Media Protection	Media includes all portable media: CDs, DVDs, Thumb Drives, Flash Drives, Laptops, Cell Phones, IPADs, Netbooks, Tablets		
Encryption or EndPoint protection	30	All laptops are being encrypted; mobile devices will be encrypted by year end. Encryption of portable media today is not done; it is left to the end user.	Appendix V - General Storage
Remote "wipe" capabilities	50	Remote wipe can be done at all mobile devices except laptops. This does not apply to portable media.	Appendix V - General Storage
Supported Devices	0	A project that will limit the SW to use in mobile devices and will allow remote wiping is in progress.	Appendix V - General Storage
Specific Configurations	60	Mobile devices have to be at the latest O.S. version to be used on network.	Appendix V - General Storage
"Controlled" Applications (Email)	25	Plan to implement secure mail technology by the end of 2017, email will be synced with server and contained to secure partition on mobile device.	Appendix V - General Storage

F. Data Classification Pitfalls to Avoid

Some of the data classification pitfalls that should be avoided are:

- Relying on narrowly defined or inconsistent data security classification policies.
- Defining more than four data security classification names.
- Selecting names that are confusingly similar or very abstract or omitting examples that illustrate each classification.
- Failing to specify the required controls for every system, content, and media type that contains sensitive information, including:
    - Structured data.
    - Unstructured and semi-structured data repositories.
    - Messaging systems.
    - Portable devices and storage media.
    - Backup tapes (during storage and transportation).
- Inadequate implementation of the required controls.

The biggest pitfall is failing to move forward with implementation, after completing the data classification policy and standard.

VIII. Litigation Readiness

In the course of regular business activities, nearly all companies become the target of lawsuits. These vary from common lawsuits, such as employee wrongful termination, to major litigation, such as class action lawsuits. Likewise, companies themselves initiate litigation. Litigation always has been, and will continue to be, a reality of doing business. What has changed, however, is the nature of litigation discovery, and the now almost complete focus on various types of electronically stored information (ESI). New requirements and technologies are changing the expectations of both parties to litigation as well as the courts, and increasing the risks and costs for companies that are not prepared.

While the timing, breadth, and frequency of the litigation is often beyond the control of companies, getting ready to manage this inevitable event is something for which in-house counsel can and should prepare. This section outlines the benefits of replacing a reactive, ad-hoc discovery process with a proactive litigation readiness program that can substantially reduce the risks and costs of implementing legal holds, collecting relevant ESI, and otherwise responding to eDiscovery requests.

A. Proactive Litigation Readiness vs. Reactive eDiscovery

Waiting for litigation to occur can be both risky and expensive – especially for companies with high litigation profiles. Because of their urgency, responding to discovery and placing legal holds can disrupt business operations and consume available resources, making it hard for a company to get out of the reactive discovery mindset. Instead of waiting for discovery requests to appear, organizations need to anticipate and prepare for future litigation requirements.

An important goal of an information governance program is to develop proactive processes and procedures that lower risk and reduce cost, and implement them outside the glare of matter-specific discovery. An investment in proactive information management will have a much bigger impact in terms of cost savings than attempting to make a reactive eDiscovery process more efficient.

The first and most critical stage of litigation discovery – the identification and preservation of potentially relevant documents and information – depends on counsel's ability to recognize the obligation, and to issue timely and effective legal hold notices to information custodians. The timing and scope of a legal hold are critical; if counsel misjudges either, sanctions, or even adverse verdicts, can result. As described below, a proactive Litigation Readiness program can help reduce the risks and costs that might otherwise be associated with delayed action or incomplete execution of a legal hold.

Once an effective legal hold is in place, the subsequent stages of eDiscovery – including collection, processing, review, and production – also present risks and obligations for corporate counsel, as well as significant opportunities for reducing enterprise risks and discovery costs, through both good information governance practices and the strategic use of culling technologies. As part of its overall IG roadmap, a company should consider developing a Discovery Response Plan (DRP) that guides corporate counsel (and other stakeholders) in the consistent and repeatable planning and execution of each stage in the process. Additional steps, as outlined below, include selection and preparation of witnesses who may need to testify during depositions or discovery conference proceedings and the application of appropriate technology tools to support cost-effective review and production of ESI during the discovery process.

It is worth noting that other components of an IG program can multiply the savings achieved by more efficient discovery response processes. As the amount of redundant, obsolete, and trivial data it retains is reduced (decreasing its total data footprint), the company can, thereby, reduce the amount of data that must be preserved and processed in response to litigation needs over a period of years. The potential eDiscovery cost savings can provide powerful motivation for a litigation readiness initiative, especially in litigation-intensive environments.

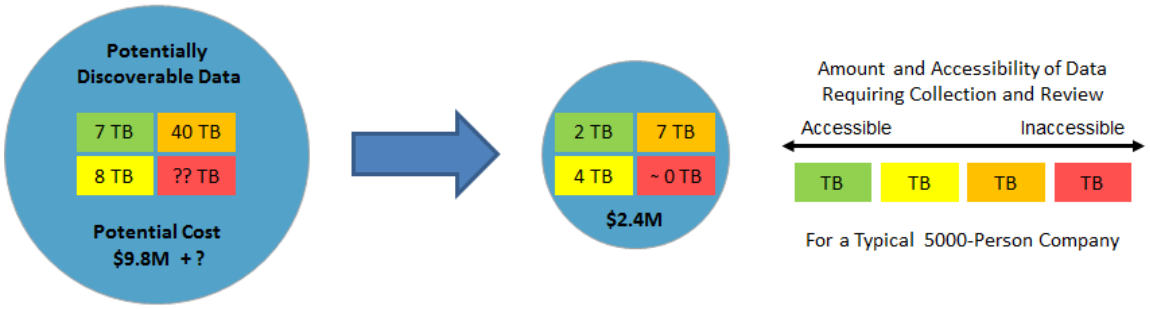
While it is practically impossible to forecast the extent and timing of future legal matters over a period of years, most organizations do have information about their past litigation experience that can help develop metrics pertinent to likely litigation costs. The resulting cost metrics can provide both motivation and justification for near-term projects to improve eDiscovery processes and tools. As previously discussed, these cost metrics can also provide important inputs to an IG program ROI model, enabling the model to support a broader range of IG investments by estimating the resulting savings in litigation discovery costs over a period of several years.

The annual costs of eDiscovery can be quite large, even if a company experiences only a few large matters in a given year or a significant number of medium-size matters on an annual basis. Many organizations, however, often find it difficult to obtain a complete accounting for the true costs of all litigation matters across the enterprise. This includes not just the costs of hiring outside counsel and paying settlements or judgments, but the in-house hard and soft costs associated with eDiscovery response. To supplement the internally-generated cost metrics, it is useful to consider estimates from published benchmark studies and from sources that can aggregate the cost across a number of companies and cases. For example, a study by the Rand Institute reported median eDiscovery costs of $1.8 million per case).[7]

While more efficient discovery processes can reduce the costs of eDiscovery for each Gigabyte of data that enters the discovery process, an effective IG program can multiply those process-related savings – both by reducing the amount of data that needs to be processed in the first place and by making the retained data more accessible.

Shrinking the enterprise data footprint not only provides easier access to information, it also significantly reduces the costs and time required for collection, review, processing, and production. Therefore, truly effective discovery cost reduction starts with better information management and disposition practices, implemented through an overall IG program.

For example, consider the following illustration for a 5,000-person enterprise. The total corporate data footprint initially exceeds 55 Terabytes and the implementation of an effective IG reduces that total footprint to 13 Terabytes. Moreover, after implementation of a data placement strategy (DPS) that improves the company's ability to find and manage information, a much smaller percentage of the data is located in repositories that are difficult and expensive to search for business operations or for litigation discovery.



Given the initial 55 Terabyte corporate data footprint, this company's conservative cost model estimates that a large litigation matter will generate $9.8 million in eDiscovery costs. However, after an IG program shrinks the corporate data footprint, and makes that data easier to find and process, the estimated cost of a similar matter drops to $2.4 million. Since the company's litigation profile indicates multiple large medium-sized matters over its five-year planning period, the estimated savings in discovery costs exceed $10 million over that timeframe.

In addition to reducing the direct costs of eDiscovery as illustrated above, an effective IG program can also reduce spoliation risk by facilitating rapid and effective implementation of legal hold procedures. Moreover, faster assessment of reduced data and information sets can enable early and well-informed decisions about optimal case strategy.

It is worth noting that these litigation-related cost savings and risk reductions are incremental to the other annual operating savings an organization can realize by shrinking its data footprint. Those operating savings include reductions in the predictable annual costs of data storage and information management, and improvements in employee productivity. For an enterprise with a high litigation profile, however, the savings in litigation costs can actually exceed the savings in storage and operating costs,

B. Legal Hold is the Crucial Step

At a minimum, a defensible discovery response plan should include a well-defined process to issue and manage a legal hold at the onset of litigation. Once a Legal Hold Notice has been issued, relevant records must be preserved and protected from both destruction and alteration until the hold is released.

Thus, the first and most critical stages of litigation discovery are the identification and preservation of potentially relevant documents and information. The timing and scope of a legal hold can differ from case to case, and almost always involves the reasoned judgment of in-house counsel about whether a set of circumstances triggers the preservation obligation. A proactive Litigation Readiness program can help in-house counsel work through this process – and reduce the risks, sanctions, and cost increases that might otherwise be associated with delayed action or incomplete execution of a legal hold.

Improving readiness for effective legal hold should, therefore, be a major short-term objective of an IG program. This section reviews key requirements for issuing and maintaining a legal hold, and some of the issues and implications corporate counsel and other stakeholders need to understand when dealing with legal hold requests. Additional procedural considerations are part of a formal Discovery Response Plan, discussed below.

1. The Duty to Preserve Starts Early

As experienced in-house counsel know, the duty to preserve relevant information starts when notice is received or when a lawsuit could be "reasonably anticipated." Courts have ruled that the duty to preserve documents relevant to litigation begins when companies "knew or should have known" that litigation was imminent. Since 2003, when Judge Scheindlin issued the groundbreaking decisions in the case of *Zubulake vs. UBS Warburg*, the requirements for legal hold have been established and expanded through additional clarifying case law. Similar preservation obligations also apply to regulatory examinations and grand jury investigations.

As soon as a company enters litigation – or has a reasonable belief it will enter litigation – it must take steps to enact a legal hold, ensuring that all documents relevant to the litigation will be preserved. While legal hold notices are often directed to individual custodians of documents and information, corporate counsel will also expect the IT organization (and designated repository custodians) to be able to preserve electronic documents effectively in the systems and repositories they control.

2. Spoliation Can Be Costly

A failure to issue a timely legal hold notice, or to quickly implement its requirements, can expose a company to fines, sanctions, adverse jury instructions, and unfavorable case

outcomes. "Spoliation" is the term used by courts to describe the improper destruction of evidence – including documents, email, messages, and other electronically stored information (ESI).

Companies can be found responsible for spoliation if they destroy evidence (e.g., company records or other information) that is relevant to the litigation with the purpose or intent of preventing the other party from using the evidence against them. Spoliation can occur actively (e.g., someone shreds documents or deletes email messages, knowing they are relevant to a case) or passively (through not following the right processes).

Spoliation, unfortunately, is not always a case of someone consciously deciding to delete evidence. Many cases of spoliation result from the failure to take actions that would have prevented the destruction of potentially relevant documents or information.

For example, spoliation could include an IT department's failure to stop backup tape rotation procedures that overwrite the existing data or the action of reformatting the laptop from a former employee for a new employee. Counsel should instruct IT administrators and other custodians to halt immediately all document deletion programs and procedures with regard to potentially relevant information when a business learns there is a reasonable probability of a lawsuit, regulatory inquiry, or government investigation.

Recent amendments to the Federal Rules of Civil Procedure have made it slightly more favorable for companies who negligently or accidentally delete relevant information as the new rules require nearly intentional conduct to warrant sanctions. The rule changes, however, do not excuse companies for having IG programs that are poorly designed, implemented, or maintained. The failure to apply reasonable and effective controls can still have significant negative consequences for companies and for counsel.

3. Legal Holds Can Impact Past and Future Data

When a litigation matter involves a specific past event or transaction, a well-framed discovery request will explicitly state the timeframe in terms of the earliest and latest document dates that are covered by the request. Counsel can then frame the legal hold notice in terms of the requested timeframe. Depending on the situation, the required legal hold and discovery timeframes can go back several years.

In other cases, the discovery requests – and legal hold notices – may cover all documents and messages that contain relevant content or that involve certain individuals or departments without a specified time frame. In the absence of an effective IG program, the scope of legal hold and discovery in such cases could include obsolete data that has been retained for many years or even decades in historical systems and storage media.

When a litigation matter could involve ongoing behavior or actively changing data sets, the legal hold may effectively require preservation of new records and information as well as pre-existing documents and data. Furthermore, an organization may need to impose multiple, cascading legal holds that apply to a given document, custodian, or repository.

Multiple and cascading holds can become particularly burdensome if the relevant documents and data have been stored on the same media or otherwise commingled. In such cases, the organization may need to retain all of the documents for a very long time, i.e., until all the holds have been released for all the affected documents.

In terms of litigation readiness, one goal of an IG program is to place documents and data into systems and repositories that enable counsel and custodians to effectively and efficiently apply, track, and release all applicable legal holds.

4. All Repositories Can Be Deemed Accessible

A legal hold applies to relevant data no matter where it is located, including legacy repositories or backup tapes that have not been touched for years. In the past, parties were able to argue that such ESI was "inaccessible," and would cause undue expense and/or hardship to retrieve. As technology has improved, the "accessibility" defense has become less about the difficulty to retrieve older information from obsolete systems and more about the cost of doing so. If the data can be accessed – even with great difficulty or at high cost – then the court may consider, in its decision about whether to allow such discovery, the likely impact of the information, the estimated costs of retrieving and producing the data, and the equitable allocation of those costs among the parties.

5. Defining an Effective Legal Hold Process

Keeping in mind the requirements and issues outlined above, corporate counsel should work with appropriate stakeholders and resources to identify likely custodians and repositories and then initiate and manage each step in the Preservation phase of eDiscovery.

- Draft a written legal hold notice [*see Writing the Legal Hold Notice* below].
- Send the legal hold notice to the identified custodians.
- Track and monitor legal hold notice responses to ensure that every custodian acknowledges the notice.
- Send reminders of the legal hold, while it is in place.
- Monitor actual compliance with the legal hold notice.
- Update the legal hold notice if the scope of discovery changes.

- Release the legal hold when all discovery obligations are satisfied.

Consistent adherence to the complete process, and documentation of each completed step, will help ensure that the preservation process is effective and defensible in the event a party's actions are ever called into question by the court.

For individual record custodians, the legal hold process may require an interview to determine the extent to which an employee has access to relevant records, and the repositories in which they are stored.

A good legal hold process will also include effective methods for establishing and tracking the custody of the material that has been placed on hold, whether that material is retained in its original locations, or immediately collected and stored separately to ensure its preservation and integrity.

Finally, a process must be put in place to handle discovery requests against the body of held records.

A documented procedure, standard templates, and forms or electronic tracking and management systems must support each of these elements. Appropriate training for litigation support staff, company managers, and employees is also needed.

As part of an overall IG program, a company should complete an assessment of its documented legal hold process – and its actual preservation practices – in terms of the requirements outlined above. An assessment would include the following steps:

- Start by determining the amount and variety of information under management.
- Identify data sources with possible litigation impact and the systems used to create and store them.
- Review existing legal hold processes for major and minor matters.
- Evaluate risk exposure levels and responsiveness gaps.

Depending on the findings of this assessment, the company can develop enhanced procedures and tools for consistent and defensible legal hold notice management and tracking, including:

- Identification of custodians and potential legal hold triggers.
- Repeatable decision processes for issuing legal hold notices.
- Methodologies and tools for identifying and locating information pertinent to a legal hold.

Good legal hold processes require close cooperation between corporate counsel, IT teams, and records custodians.

6. Writing the Legal Hold Notice

Corporate counsel should prepare and issue the legal hold notice in written form. While the format and content of the notice may vary (depending on the facts and circumstances), the written communication to custodians should contain the following elements:

- Date issued.
- Identity of the issuing authority.
- Reason for the notice or order.
- Scope of the legal hold notice.
- Specific, explicit instructions to preserve and not delete, modify, or alter all relevant information, including ESI.

The "scope" of the notice should cover:

- Employees (and other custodians) covered by the notice.
- Types of records and information and any specific content.
- Timeframe covered.
- Locations of information under hold.
    - Listing of applicable systems, repositories, and media types.
    - Potential employee home workstations.

Some have questioned the need for a written legal hold. In 2010, Judge Sheindlin opined that anything less than a written legal hold was gross negligence:

> "Courts cannot and do not expect that any party can meet a standard of perfection. Nonetheless, the courts have a right to expect that litigants and counsel will take the necessary steps to ensure that relevant records are preserved when litigation is reasonably anticipated, and that such records are collected, reviewed and produced to the opposing party . . .[However,] the failure to issue a WRITTEN legal hold constitutes **gross negligence** because that failure is likely to result in the destruction of relevant information."
>
> -- Judge Shira Sheindlin, *Pension Committee v. Banc of America Securities*, Amended Order, No. 05-cv-9016 (emphasis added)

Subsequent opinions moderated this ruling, with most courts finding that the need for a written legal hold depends on the facts and circumstances of each individual matter. For additional considerations and context, see the following case examples:

- Rimkus Consulting Group v. Cammarata (S.D. Tex. 2010).
- Victor Stanley v. Creative Pipe (D. MD. 2010).

- Steuben Foods v. Country Gourmet Foods (W.D.N.Y. 4/21/2011).

Regardless of case law, documenting a legal hold provides a more defensible process. Discovery disputes often occur months or years after issuance of the legal hold, as well as the discussions around preservation obligations. A written legal hold – as well as documentation of the entire process – will help defend those decisions, should they be called into question in the future by the opposing party or the court.

C. Who Is Driving the Discovery Car – In-house or Outside Counsel and Vendors?

Traditionally, when medium and large litigation or regulatory inquiry strikes, in-house counsel have engaged law firms or eDiscovery providers to manage the discovery process. Many companies, however, have learned the hard way that they should still supervise and, in some cases manage and control, all phases of the eDiscovery process in order to control costs as well as risk. Allowing outside counsel and eDiscovery vendors to "drive" the eDiscovery process without proper oversight can result in high collection and processing costs, and ultimately high review costs from outside counsel.

1. Professional Ethics Rules Require Competence

Recent amendments to the American Bar Association Rules of Professional Conduct now state that lawyers have a responsibility to understand the technology that is used in furtherance of serving their clients:

- A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. (ABA Model Rule of Professional Conduct 1.1.)
- To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. (Comment 8, Rule 1.1.)

In-house counsel must understand the capabilities, limitations, and appropriate uses of the technology tools that are used in the identification, preservation, and collection of ESI for litigation. Counsel must also maintain adequate understanding of the technologies that control retention and disposition of company records in support of proper IG practices and outcomes.

The new rules make clear it is no longer enough for in-house counsel to delegate responsibility for eDiscovery to outside vendors or even outside counsel. Nor is it necessary for in-house counsel to become "IT experts" with an intimate understanding of how each and every corporate system works. To play a meaningful part in the eDiscovery process, in-

house counsel must have a reasonable understanding of the organization's information systems, in order to properly advise outside counsel when negotiating the scope of discovery, as well as with outside vendors, in order to make sure collections are targeted and costs controlled.

2. Responsibility Cannot Be Delegated

Courts repeatedly hold that in-house counsel cannot delegate responsibilities to outside parties or even to regular employees of the organization, and they routinely impose sanctions in cases where in-house counsel failed to properly direct and control eDiscovery processes.

In *Qualcomm v. Broadcom*, the court found that in-house counsel is not absolved from participating in eDiscovery once outside counsel is hired.[8] In that case, Qualcomm failed to produce certain relevant documents, the existence of which was known to outside counsel but not to Qualcomm lawyers. The organization was sanctioned for discovery misconduct, forced to produce additional documents, and several in-house lawyers were subject to disciplinary proceedings.

Furthermore, counsel cannot simply delegate its eDiscovery responsibilities to the company's employees - such as custodians and IT teams – without proper oversight or control. In *Green v. Blitz USA, Inc.*, the company appointed its manager in charge of product design (who admitted he knew little about computers or technology) to search for and produce relevant documents related to a claim of defective design.[9] As a result, Blitz was heavily sanctioned for failing to produce relevant ESI.

3. Getting Control of eDiscovery Risks and Costs

In addition to the professional requirements and the risks of sanctions or adverse decisions, corporate counsel must avoid the high costs of excessive collection and processing by outside vendors -- and the resulting increases in review costs as well.

In-house counsel need to develop and maintain sufficient knowledge and expertise to manage an outside vendor. Counsel must not allow the vendor to drive the discovery strategy, as well as its execution without some level of oversight and control. While most vendors will be reasonable, there is, of course, a motivation to collect as much information as possible and to store that information as long as they can manage to charge for doing so. To properly control discovery costs, corporate counsel must 1) work to limit the scope of data collected by the vendor and 2) understand the processes and the implications of storing the proposed volumes of collected data. Outside vendor activities should be part of

any DRP. Once that plan is in place, counsel must monitor and audit outside vendor activities on an ongoing basis.

If an outside vendor is allowed to propose and execute a strategy that collects excessive volumes of data, the collection and hosting of that data can become very expensive. Costs can escalate even further when outside counsel proceeds to review those excessively large volumes of data. Technology can be used to reduce the volumes of collected data, and the costs of using this technology must be considered as well.

The goal in any legal matter should be to negotiate a reasonably narrow scope of discovery. This scope should discourage "fishing expeditions" and monitor and control the execution of the collection, processing, and review phases.

By supporting and participating in a comprehensive IG program, and from a more strategic perspective, corporate counsel can move to control eDiscovery budgets more effectively. This helps to ensure there is a small data footprint from which the vendors can collect.

Note that a well-developed DRP typically includes a Discovery Conference Preparation Guide, which provides basic tools and information for use by outside counsel when preparing for a Meet and Confer or other discovery conference, as well as basic information outside counsel needs to know about how the organization conducts eDiscovery. The document helps ensure that outside counsel is able to adequately represent the company's eDiscovery mechanisms and processes, and to negotiate a reasonable scope of discovery.

D. Creating a Coordinated In-house Discovery Response Plan

As part of an IG roadmap, a company should consider developing a Discovery Response Plan that guides corporate counsel and other stakeholders in the planning and execution of each stage of the discovery response process.

A coordinated, well-documented DRP:

- Addresses all phases of the Discovery process.
- Establishes and utilizes a Discovery Response Team for both strategic and tactical management of discovery in legal matters.
    - Team includes key members from Legal, IT, RM, Compliance.
    - Engaged to mitigate costs of over-broad Legal Holds and collections.
- Includes guidelines, workflows, and templates for legal hold distribution, acknowledgment, refresh, and release.
- Includes forms for collection and processing phases, including Chain of Custody documentation.

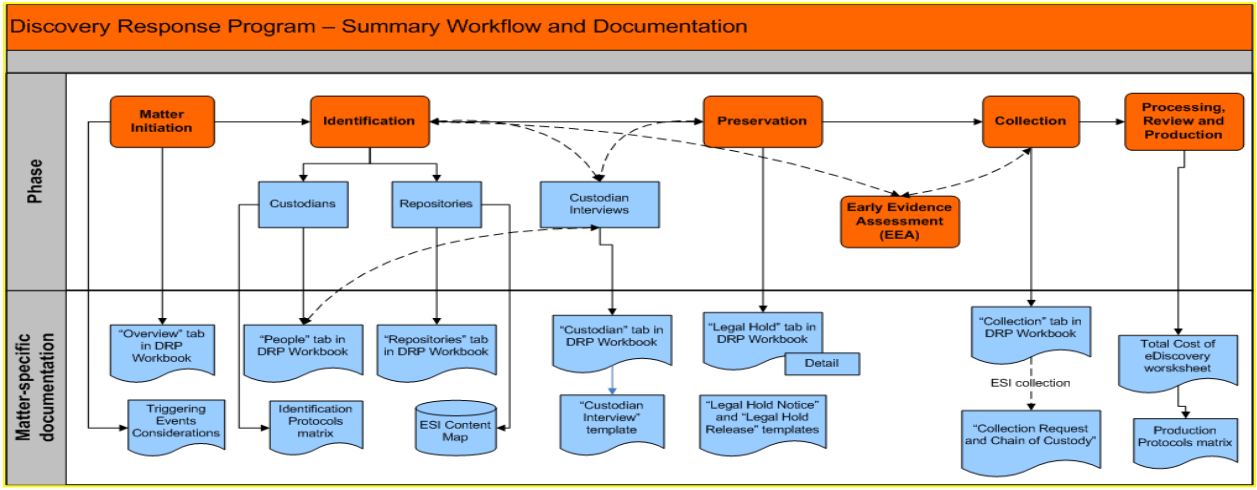
- Provides a defensible and consistently followed process with metrics, auditing, and routine data reduction.

The DRP should be customized to address an organization's litigation profile, and reflect industry best practices, as well as the company's needs and resources (in the context of typical litigation and regulatory examination scenarios).

A DRP also should define the appropriate roles for in-house legal staff and outside counsel and/or discovery service providers, including responsibilities for:

- Collection of electronic data and paper records from individual custodians and IT-managed repositories.
- Preservation and chain of custody.
- Filtering and de-duplication.
- Review, redaction, and production.

The DRP should include workflow diagrams to demonstrate discovery phases and a summary workflow to show how all phases fit together.



Within that overall context, the DRP should also include a detailed procedural section for each phase of discovery, showing required process workflows and describing the appropriate forms, templates, tracking logs, and other documentation. It should also address, where appropriate, potential exceptions and alternate procedures or tools. The following is a very basic outline of steps to take as part of an overall discovery response process:

Litigation Discovery Phases	
MATTER INITIATION	Conduct initial preservation meeting with the discovery response team.

	Analyze whether preservation obligations have been triggered.
	Immediately assess the company's preservation obligations.
	Create a preservation strategy.
IDENTIFICATION	Identify documents or categories of documents to be preserved.
	Develop a list of key custodians or business units.
	Develop a list of repositories and IT custodians.
PRESERVATION	Draft the Legal Hold Notice (preservation notice).
	Issue the Legal Hold Notice.
	Track and monitor Legal Hold Notice responses.
	Monitor compliance with the Legal Hold Notice.
	Update the Legal Hold Notice as appropriate.
	Release the Legal Hold.
COLLECTION	Develop and document the collection plan.
	Implement the collection plan, and document the collection activities.
	Refresh the collection, as necessary.
PROCESSING	Internal teams and/or outside vendors: Cull, de-duplicate, and otherwise reduce the volume of information gathered in the collection phase.

REVIEW	Legal teams (typically law firms): Review the processed information.
	Determine what is relevant and must be provided to opposing counsel (or to regulators).
	Remove data that is not relevant.
PRODUCTION	Outside counsel and/or authorized vendors: Prepare the data for delivery to opposing parties (or to regulators).

E. Selecting and Preparing a Rule 30(b)(6) Witness

An understanding of eDiscovery – as well as the establishment of policies and processes for records retention and legal hold – will reap enormous benefits, and additional steps can be taken to further prepare for litigation. During the discovery phase, opposing counsel often issues a request to learn more about an organization's information systems, to prepare them for framing an appropriate discovery request. Employees who can testify on this subject should be designated and trained for this role. In fact, rather than designating someone on a case-by-case basis, a good practice is to have qualified witnesses identified and trained on how to provide testimony ahead of time. Adjustments can be made for the individual legal matter and its particular circumstances.

As part of the Meet and Confer or discovery conference proceedings, organizations should be prepared to answer specific questions about their data and where it is located within the IT infrastructure. For ESI, organizations are encouraged to designate and prepare a specific individual (or individuals) who will be able to testify about the ESI produced during the discovery. Some concerns and questions this witness can expect during a deposition include:

- The location and storage of documents subject to disclosure.
- Details about specific system applications, including e-mail systems, enterprise applications, databases, document imaging systems, among others.
- Details about servers and infrastructure.
- E-mail and data backup and restoration policies, practices, procedures, and schedules (including media and software used and storage locations).
- Search methodology and use of electronic search to locate relevant electronic documents.
- Who are the custodians of these systems?

- What is the retention policy for each system?
- Who is responsible for retention periods for these systems?
- What are the backup policies and practices?
- What data is inaccessible or unduly difficult to recover?

Companies should identify their designated witnesses well before litigation strikes. This can be someone in IT or a business unit that understands the data, and it is important that the designated person be well versed in the IT infrastructure and the applications that create and manage information. The best Rule 30(b)(6) witness is one who is dispassionate and reasoned while still well-informed. Different individuals may be required, depending on the types of data and the repositories that may be relevant to a specific matter or specified in a discovery request.

If the company has a data map, as previously discussed, it can help counsel identify the appropriate Rule 30(b)(6) witness for particular repositories and the data map can also be used when preparing the witness to testify.

In preparing a 30(b)(6) witness for deposition, in-house counsel should, of course, provide the guidance normally given to any deposition witness, including advice to:

- Speak in short, succinct sentences.
- Not volunteer information.
- Speak slowly and audibly.
- Think before speaking.
- Ask for clarification if the question is not understood.
- Review all documents carefully.
- Be professional and polite.
- Most importantly, always tell the truth.

F. An Overview of Predictive Coding and Data Analytics

For many years, eDiscovery experts have wrestled with the fact that human review of ESI takes too long and the volume of relevant ESI continues to grow exponentially in the average legal matter. To make the review process more efficient, eDiscovery vendors developed "predictive coding" technologies, which can review large volumes of information in a short period of time, and identify relevant documents based on information provided by subject matter experts. The more commonly-used term today is Technology Assisted Review (TAR), which refers to computer applications and techniques

that outside counsel and eDiscovery vendors employ to enable review of large volumes of documents and data, with greater speed and substantially lower costs.

In the IG area, auto-classification approaches have seen very limited success and acceptance. Many companies are hesitant to trust that an auto-classification tool will correctly identify a document's content and assign the proper retention period to it – the failure of which would lead to the inadvertent early deletion of that record. With eDiscovery, the risk of improper classification does not carry the same consequences and, as a result, TAR is becoming more widely accepted in litigation discovery and is now routinely approved (or sometimes even expected by courts as standard practice) in federal courts and many state jurisdictions.

The acceptance of TAR reflects the nature of the problem. In litigation discovery, the application is required to place a document into one of two categories. On the first pass, documents are classified as relevant or not relevant to a specific matter. On a second pass, a fraction of the relevant documents may be further classified as privileged, for purposes of production to opposing counsel. Multiple studies have demonstrated, to the satisfaction of most courts, that TAR applications now produce results as good as, or better than, traditional labor-intensive human review approaches.

G. Other IG Activities That Will Drive Litigation Readiness

To achieve significant cost savings and risk reduction, enterprises should commit to establishing control over information *before* the next legal action. In short, when it comes to litigation readiness, a good offense is the best defense. This section highlights three components of an IG program that can significantly enhance litigation readiness.

1. ESI Data Map

Counsel should consider working with IT to build a map of the data sources that might be subject to legal hold. The resulting map can be used by counsel during early case assessment, meet and confer, discovery scoping, and response planning.

As previously noted, an organization may construct a data map for one or more purposes and use cases. In the context of litigation discovery, an enterprise may benefit from a data map that is specifically designed or adapted to meet the needs of in-house litigation counsel.

The data map can provide useful capabilities for key tasks in several phases of the process. Typical examples include:

- Identification of repositories that are likely to contain the requested documents and data – in terms of content types, date ranges, and usage.
- Identification of custodians who control relevant repositories or who have access to the contents of those repositories.
- Maintenance of up-to-date descriptive information on each repository, which can enable timely and accurate responses in discovery meet and confer conferences.
- Identification of suitable Rule 30(b)(6) witnesses and support for preparation of those witnesses prior to scheduled depositions.
- Early assessment of the volume of data that is stored in relevant repositories.
- Rapid implementation of a legal hold, using processes and tools that have been identified in advance as the most appropriate and effective methods for specific repositories.

2. Data Placement Strategy

By developing and implementing a comprehensive Data Placement Strategy (DPS), a company can make its data easier to find, hold, collect, and process during the phases of a single litigation matter. During implementation of the strategy, as part of the overall IG roadmap, the enterprise can place various types of documents and data into systems and repositories that provide the appropriate configurations, capabilities, and controls for management and disposition of each type of data.

When developing its DPS, an organization should also specify capabilities and controls that can support all the needed processes for each phase of an effective and efficient litigation discovery process and Discovery Response Plan implementation.

3. Defensible Disposition

In compliance with its Records Management Policy and Records Retention Schedule, a company should establish defensible disposition processes for records and for non-record information.

In the context of litigation discovery, defensible disposition processes can reduce the risk of actual spoliation. If requested documents or data are found to have been deleted (in the normal course of business) prior to the onset of litigation, such policies and processes can help a company establish an effective defense.

A defensible deletion process:

- Is supported in the records retention policy.

- Utilizes the RRS to identify records to be saved in compliance with legal, regulatory, and business requirements.
- Requires strong legal hold processes.
- Must be monitored and audited to be effective.

IX. Final Thoughts: Dealing with Imperfection

Historically, a large part of launching a records management program was the development of a records retention schedule. Recordkeeping was a straightforward process when most records were created and stored on paper. Then the world changed. Information switched from paper to electronic media. Recordkeeping regulatory requirements increased. Companies faced new requirements, such as privacy. Data began accumulating. eDiscovery demands increased. The simple job of records management became more difficult.

Today's environment poses a number of legal, compliance, regulatory, privacy, breach, and eDiscovery risks, and in-house counsel worry about how to protect and defend their clients in this new landscape. Records management programs are combining with privacy, eDiscovery, and IT initiatives and becoming full-fledged Information Governance programs. These newer programs are larger and more complex, and they put more burden on in-house counsel and other key stakeholders to govern their information legally and defensibly.

In-house counsel may ask themselves: how do we know we have it right? They start looking for the *perfect* policy, the *perfect* process and the *perfect* tool. We are not ready to start, they tell themselves, because we are not quite there yet. In the meantime, documents and data accumulate, requirements become stricter, and risks increase. *Perfect* becomes the enemy of "good enough" (i.e., reasonable).

Information Governance is an inherently imperfect process. Fortunately, the courts and regulators do not expect perfection. Rather, they expect reasonable good faith efforts. In your policies, declare what will be done. Execute those policies with processes, technology, and training. Demonstrate that policies are being complied with through metrics and audits. Show that a plan has been developed. Show that the plan is being executed. Audit the results and remediate any shortfalls. Not perfect? That is OK. No one expects it to be perfect. Start with good and just keep moving forward.

X. About the Author

A. About Contoural, Inc.

Contoural is the largest independent provider of strategic Information Governance consulting services. We work with more than 30 percent of the Fortune 500 and numerous mid-sized and small companies, and provide services across the globe. We are subject matter experts in Information Governance, including traditional records and information management, litigation preparedness/regulatory inquiry, information privacy and the control of sensitive information, combining the understanding of business, legal and compliance objectives, along with operational and infrastructure thresholds, to develop and execute programs that are appropriately sized, practical and "real-world". Contoural is also the 2016 co-sponsor of ACC's Information Governance Committee.

Contoural is an independent services provider exclusively focused on Information Governance consulting services. Contoural sells no products, takes no referral fees from product vendors, nor provides any "reactive" eDiscovery, document review or document storage/warehousing services. This independence allows us to give our clients unbiased and impartial advice while serving as a trusted advisor.

With an average of 24 years of experience, Contoural consultants include former litigators, former in-house counsel, records managers, compliance experts, eDiscovery specialists, privacy professionals, technology experts, former CIOS, training and behavioral change management specialists, industry technology analysts, among others. Many hold JD degrees; most are members of ARMA International, IAPP or AIIM, and most have in-depth experience in one or more areas of technology that can help enhance, and potentially automate, the implementation of policies, retention schedules, and processes for records management and litigation readiness. In addition, Contoural consultants remain active in the legal community, including the American Bar Association and various State Bar Associations.

Contoural services include:

- Assessment and Roadmap Development
- Record Retention Policy and Schedule Creation and Update
- Data Security Classification
- Litigation Readiness
- Data Placement

- Technology Selection
- Taxonomy and File Plan Development
- Behavior Change Management and Training
- Legacy Document and Data Remediation
- Information Governance Organizational Development.

B. About the Author

Mark Diamond, President and CEO, Contoural, Inc.

Note: The content in this InfoPAK reflects the collective insight, experience, recommendations, advice, and wisdom of a number of Contoural consultants and other team members. While Mark is listed as the author, any credit for the quality of the content should be bestowed on this larger team. Any shortcomings belong exclusively to Mark.

Mark Diamond is an industry thought leader in information governance, encompassing records and information management, litigation readiness, control of privacy and other sensitive information, defensible disposition, and employee collaboration and productivity. Mark is a frequent industry speaker, presenting at numerous Legal and IT industry conferences. Additionally, Mark addresses more than one hundred internal corporate audiences each year with onsite seminars.

Mark is founder, President & CEO of Contoural, Inc. Previously, Mark was co-founder of Veritas' (OpenVision) Professional Services group, founder and General Manager, Worldwide Professional Services for Legato Systems, Vice President of Worldwide Professional Services at RightWorks, and he has worked as a management consultant. He also served as Chair of the Storage Networking Industry Association customer advisory board on data security. He sits on the board of advisors for high technology companies.

He has a Bachelor's degree in Computer Science from the University of California San Diego. Mark is former President of the UC San Diego Alumni Association, and served as a Trustee of the university's foundation. He can be reached at mdiamond@contoural.com and for more information, on Contoural's site at http://www.contoural.com/about-management_team.php.

Mark welcomes any questions or comments on this InfoPAK.

XI. Additional Resources

A. ACC Docket Articles

Annie Drew and Mark Diamond, "Building a Business Case for Information Governance," *ACC Docket* 32, no. 8 (Oct. 2014): 26-40, *available at* http://www.acc.com/legalresources/resource.cfm?show=1377595

B. Contoural Whitepapers

"Defensible Disposition: Real-world Strategies for Actually Pushing the Delete Button" *White Paper,* (2014), *available at* http://www.contoural.com/whitepaper_summary.php?id=31

"Metrics Based Information Governance," *White Paper,* (2013), *available at* http://www.contoural.com/whitepaper_summary.php?id=28

"Stop Hoarding Electronic Documents," *White Paper,* (2012), *available at* http://www.contoural.com/whitepaper_summary.php?id=32

"Email Classification Strategies That Work," *White Paper,* (2012), *available at* http://www.contoural.com/whitepaper_summary.php?id=29

"Migrating and Decommissioning Legacy Applications," *White Paper*, (2014), *available at* *http://www.contoural.com/whitepaper_summary.php?id=30*

"Seven Essential Storage Strategies," *White Paper*, (2015), *available at* *http://www.contoural.com/whitepaper_summary.php?id=1*

"Is It Time for Auto-Classification? – Part 1," *White Paper*, (2015), *available at* http://www.contoural.com/whitepaper_summary.php?id=3

"Is It Time for Auto-Classification? – Part 2," *White Paper,* (2015), *available at* *http://www.contoural.com/whitepaper_summary.php?id=2*

D. Other Articles

Mary Butler, "IG and 'Mission Control': Launching the Future of Healthcare," *The Journal of AHIMA*, (2015), *available at* http://journal.ahima.stfi.re/2015/08/01/ig-and-mission-control-launching-the-future-of-healthcare/?sf=pkyvo#aa

Mary Butler, "Panel: launching Information governance harder than Landing on the Moon," *The Journal of AHIMA*, (2015), *available at* http://journal.ahima.org/2015/05/18/panel-launching-information-governance-harder-than-landing-on-the-moon/

Melissa Maleske, "4 Ways GC's Can Better Control Their Data," *Law360*, (April 28, 2015), *available at* http://www.contoural.com/docs/4%20Ways%20GCs%20Can%20Better%20Control%20Their%20Data%20-%20Law360.pdf

Mark Diamond, "Eight Steps in Launching an Information Governance Program," *Compliance and Ethics Professional,* (March 2015): 17-21, *available at* http://www.contoural.com/docs/scce-cep-2015-03-Diamond.pdf

John Mancini, "How to get Serious About Information Governance," *AIIM: The Digital Landfill* (July 2, 2015), *available at* http://info.aiim.org/digital-landfill/how-to-get-serious-about-information-governance

Mark Diamond, "Six Steps for Creating a 'Super Data Map,'" *Information Management,* (2014): 28-32, *available at* http://imm.arma.org/publication/frame.php?i=224033&p=34&pn=&ver=flex

Mark Diamond, "Can Legal and IT Agree on Compliance? Yes, And Five Steps to Get There," *CIO Review Magazine*, (December 10, 2013), *available at* http://www.cioreview.com/magazine/Can-Legal-And-It-Agree-On-Compliance-Yes-And-Five-Steps-To-Get-There-XGOO67982021.html

Mark Diamond, "The Root Cause of Washington Gridlock? Relational Databases," *Inside Counsel Magazine*, (November 2013), *available at* http://www.insidecounsel.com/2013/11/01/the-root-cause-of-washington-gridlock-relational-d

Mark Diamond, "Fibs Your e-Discovery Vendor and Law Firm May Tell You – Part 1," *Inside Counsel Magazine,* (May 2013), *available at* http://www.insidecounsel.com/2013/05/15/fibs-your-e-discovery-vendor-and-law-firm-may-tell

Mark Diamond, "Fibs Your e-Discovery Vendor and Law Firm May Tell You – Part 1," *Inside Counsel Magazine*, (May 2013), *available at* http://www.insidecounsel.com/2013/05/01/fibs-your-e-discovery-vendor-and-law-firm-may-tell

Mark Diamond, "5 Strategies to prevent Runaway Legal Fees When Being Billed Hourly," *Inside Counsel Magazine*, (April 2013), *available at* http://www.insidecounsel.com/2013/04/08/5-strategies-to-prevent-runaway-legal-fees-when-be

Mark Diamond, "Cheat Sheet: 8 Strangest Lawsuits Driving the 7 Most Noteworthy In-House Career Moves," *Inside Counsel Magazine,* (April 2013), *available at* http://www.insidecounsel.com/2013/04/01/cheat-sheet-8-strangest-lawsuits-driving-the-7-mos

Mark Diamond, "Guidelines for Restarting Corporate Records Programs, *Inside Counsel Magazine* (March 2013), *available at* http://www.insidecounsel.com/2013/03/04/6-guidelines-for-restarting-corporate-records-prog?slreturn=1470024190

Mark Diamond, "6 Guidelines for Restarting Corporate Records Programs," *Inside Counsel Magazine,* (March 2013), *available at* http://www.insidecounsel.com/2013/03

/04/6-guidelines-for-restarting-corporate-records-prog

Mark Diamond, "A Records Management Checklist for Mergers and Acquisitions," *Inside Counsel Magazine,* (March 2013), *available at* http://www.insidecounsel.com/2013/03/20/a-records-management-checklist-for-mergers-and-acq

Mark Diamond, "What is Big Data and Why Should In-House Counsel Care?" *Inside Counsel Magazine,* (February 2013), *available at* http://www.insidecounsel.com/2013/02/19/what-is-big-data-and-why-should-in-house-counsel-c

Mark Diamond, "Records Management Might be a Career Dead-end, but Information Governance is Not," *Inside Counsel Magazine*, (January 2013), *available at* http://www.insidecounsel.com/2013/01/18/records-management-might-be-a-career-dead-end-but

XII. Endnotes

[1] Unpublished survey data from Osterman Research, Inc.

[2] Gartner Group

[3] Geneca Consulting Research

[4] 17 CFR 240.17a-4(f).

[5] 45 CFR 164.528.

[6] 45 CFR 164.400-14.

[7] NICHOLAS M. PACE & LAURA ZAKARAS, WHERE THE MONEY GOES: UNDERSTANDING LITIGANT EXPENDITURES FOR PRODUCING ELECTRONIC DISCOVERY (2012), http://www.rand.org/pubs/monographs/MG1208.html.

[8] 2008 WL 638108 (S.D.Cal., March 05, 2008).

[9] (E.D.Tex., March 1, 2011).