From Information Management to Information Governance: The New Paradigm

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

OVERVIEW

The explosive growth of information presents management challenges to every organization today. Retaining volumes of information beyond its legal, regulatory, or operational value increases data storage costs and strains information technology resources. Further, there is an inherent risk in retaining information beyond its legal or business retention needs when it may be subject to discovery related to litigation, audits, or governmental investigations. Added to these challenges are increasing privacy and security issues. Information containing personally identifiable information, intellectual property, or other sensitive data, if inadequately protected, is subject to cyber attack and security breach. The potential results of such a breach can be devastating — millions of revenue dollars lost, sanctions and fines levied, executives fired, and reputation and customer trust irreparably damaged.

Today's siloed approach to information management

Traditionally, distinct business functions within an organization have been designated as responsible for specific pieces of the information pie. Some functions with defined focus include the following:

- Records Management, responsible for establishing the retention rules for records, has historically emphasized the management of hardcopy records and now struggles to manage digital information, often requiring an approach that falls outside of the traditional methodologies.
- The Legal department, with a reactive focus on litigation and e-discovery needs, has often discounted "non-responsive" information from its purview.
- Information Security has focused its attention on implementing key controls for the security and protection of data, everything from access control permissions to data loss prevention tactics to breach response plans, without necessarily taking into consideration the practical business needs for that data.
- The Privacy Office is assigned the task of identifying appropriate responses, often reactive, to privacy-related issues, such as privacy impact assessments and guidance to the business regarding the use and retention of personally identifiable information, but may not consider the operational needs to use that information.

This myopic approach to managing information results in "one up" solutions that may solve the immediate problem. In the wake, though, additional problems may erupt since all aspects of managing the information were not taken into consideration. Expensive technology implementations, originally considered the magic wand, often fail since technology in and of itself is not a solution. Additional challenges created by the traditional approach to information management include:

- An unrealistic reliance on manual end-user-only methods to manage information
- Traditional retention schedules that are not applicable in the digital environment
- Large, enterprise-wide systems whose data does not always fit into the neat definition of a distinct digital document
- Inadequate budgeting of resources (time, money, people)
- The business' perception that this an "IT problem" and one that the Information Technology department needs to solve

Expensive technology implementation, originally considered the magic wand, often fall since technology in and of itself is not a solution.

Information Governance — the new paradigm

Many organizations are coming to the realization that the traditional manner of managing information in distinct silos just doesn't work in the age of explosive digital data growth and related risk. These organizations are beginning to take a broader, more holistic, and unified view of their information, recognizing information as a key asset of the organization, requiring heightened management and control.

Information, if properly managed throughout its lifecycle from creation or receipt until final disposition, is the corporate memory of the organization. It serves as the evidence of business activities, transactions, and processes that support legal and financial rights and obligations to customers, shareholders, and employees. It supports management decisions and strategic directions, and protects the organization against potentially damaging legal actions. In addition, information can provide a rich backdrop to an organization's culture and history, linking the past to the present. "Information Governance" describes this more comprehensive and integrated approach that assimilates the information interests and management needs of all parties within an organization. Not only are risks managed and information protected, but information is identified as an asset, optimizing and leveraging its value across all business functions and concerns. Information Governance clearly establishes a framework of accountability and responsibility for the management and governance of information throughout the organization, with the ultimate objectives of:

- Retention of information in compliance with regulation, operating need, and legal hold requirements
- Systematic disposition of information when it has no further legal or business value
- Improved access to and preservation of needed information for both business and legal purposes
- Protection of private and sensitive information requiring heightened security controls and oversight
- Overall contribution to the mission and vision of an organization through enhanced stewardship and governance of information assets

An Information Governance framework includes a number of key components, as described below. When orchestrated in a coordinated manner, the many moving parts of an Information Governance framework act together to move the organization forward towards achieving its overall governance objectives.

The Information Governance Steering Committee

Underscoring executive commitment to Information Governance, many organizations are establishing Information Governance Steering Committees. These committees are often structured to include four "layers" of roles and accountabilities:

Executive leadership. A senior executive of the organization sets the "tone at the top" by sponsoring the Information Governance Steering Committee. This role may be played by the Chief Executive Officer, the Chief Financial Officer, the Chief Legal Officer, or the Chief Information Officer. Often, several of these executives will share the sponsorship role. The Committee is accountable to the executive sponsors, and for ensuring the Information Governance strategy aligns with the overall corporate mission.

Inclusive representation. The Information Governance Steering Committee, to be successful, should be comprised not only of representation from the Legal, Privacy, Information Technology, and Records and Information Management departments, but representation from key business stakeholders as well. A formal charter that defines the mission and vision of the committee and defines the specific responsibilities of the committee chairman and members ensures alignment among all parties.

Working teams. While the Steering Committee is strategic in its focus, "working teams" may be designated to provide the tactical, project-related support for specific initiatives agreed upon by the Steering Committee. For example, the committee may determine the need to enhance the organization's approach to applying the company retention schedule to email, basing retention on the value of the email message itself, not the volume. The committee may then establish a working team to specifically address the technical, operational, and change management requirements to support that overall strategy.

Information stewards. Many traditional records management programs designate individuals within each department who serve as "records coordinators." These individuals are typically responsible for coordinating the boxing and transferring of hardcopy records to offsite records warehouses for more cost-effective storage. Although some paper records are still being generated, the vast majority of information is now electronic in format. Therefore, many organizations are evolving the records coordinator role into that of an "information steward," who now has the role of liaising with the working teams or Steering Committee to disseminate information or participate in Information Governance activities, focus groups, surveys, etc.

> **Information Governance Managers, Enterprise Information Directors, and Chief Data Officers are becoming increasingly common roles, with backgrounds that blend technology and compliance.**

Some organizations are taking leadership of Information Governance initiatives to the next level by developing new roles and organizational structures to meet this cross-functional demand. Information Governance Managers, Enterprise Information Directors, and Chief Data Officers are becoming increasingly common roles, with backgrounds that blend technology and compliance.

Information Governance policy

One of the inaugural tasks of an organization's Information Governance Steering Committee should be the development and adoption of an over-arching Information Governance policy that includes the scope, purpose, objectives, responsibilities, and standards for comprehensive information management throughout the organization. In addition to the over-arching Information Governance policy, other existing policies such as those that cover data privacy and protection as well as electronic communications should be re-examined and updated as needed to ensure they align with the comprehensive Information Governance policy.

In some cases, the records and information management policy can be expanded to become an Information Governance policy. In others, it makes sense to start from scratch, bringing in core components from a variety of existing policies and addressing new topics not previously considered. The important part of this exercise is to establish information as a valuable corporate asset and to put forward a framework that treats it as such.

Information mapping

It is likely that, over time, organizations have created multiple depictions of their information serving a variety of purposes. These various views of an organization's information may overlap in some instances, thereby presenting duplicate information. On the other hand, there may be some information known only to the party specifically interested in that type of information and yet other information that is not be represented at all. Possible maps of information that currently exist within any single organization may include the following:

- **Records Retention Schedules** are often developed and maintained by the Records Management department, and identify official company records and the time periods these records are to be retained in order to meet the organization's legal, regulatory, and operational requirements.

- **Discovery Data Maps** are often compiled by the Legal department to support its need to know where information likely relevant to litigation, audit, and government investigations may be located.
- **Application Profiles** may be maintained by the Information Technology function, identifying those key structured data systems under its management. Such profiles may identify the system name and owner, as well as other technical information needed by IT.
- **Information Security and Data Classification Inventories** identify systems or storage locations that contain sensitive and private data. These systems or locations are often identified by the Privacy Office or Information Security as warranting enhanced control and protection against breach or attack.
- **Privacy Data Flows** show the path that privacy and sensitive information takes from the point it is acquired from the customer or employee to the point it leaves the organization.

An organization needs a comprehensive understanding of all of its information and its related value from a number of different perspectives, including regulatory requirements, privacy and security, business criticality, and cost. Without such a comprehensive view, an organization risks falling back into the same habits of siloed information management.

One of the first directives of the Information Governance Steering Committees should be the development of an all-inclusive map of the organization's information to provide the baseline for assessing whether its Information Governance objectives are being attained. Often, the organization's record type inventory is a good place to start adding relevant fields of information regarding storage location, security classification, specific sensitive/private information contained, and how the data flows through the organization.

An organization needs a comprehensive understanding of all of its information and its related value from a number of different perspectives, including regulatory requirements, privacy and security, business criticality, and cost.

Information Governance strategy

Once the organization's information has been identified and its value defined, the next step is to conduct an assessment to determine whether the organization is following the "best practices" and standards as defined by its Information Governance policy. Based on the assessment results and the organization's overall corporate objectives, the Steering Committee can identify and prioritize key information management initiatives that will help close the gap between the current "as is" environment and the desired future state. In order to establish a consistent approach to lifecycle information management and governance, these initiatives may include:

- A strategy for the management of unstructured content, including email management systems, collaborative environments, network share drives, and document management systems, leveraging existing technology and tools where appropriate.
- A process for a risk-based assessment and remediation of structured data and source systems to meet records and information management requirements.

The development of a reasonable, time-based "roadmap" showing the sequencing and priority of the initiatives will allow the organization to move sensibly from its current state to a fully deployed and sustainable program. Immediate attention to high-risk areas will allow the organization to address critical improvements in key areas while moving forward with foundational improvements in information management technology and processes that may require several years to fully achieve.

An eye on privacy and security

"Defensible deletion" is certainly a goal of comprehensive Information Governance, since it helps ensure that only information required to satisfy regulatory, legal, and valid business and operating needs is retained. However, until information is eligible for disposition, special attention needs to be paid to it particularly if it contains personally identifiable information (PII), private health information (PHI), or other sensitive data. Generally, this information should be retained only as long as absolutely necessary; in some jurisdictions, there are statutory maximum retention periods.

Potential conflicts often arise between privacy requirements that demand that information be disposed of as soon as possible and legal or business needs to retain the information longer. It is critical that the Privacy, Legal, and business functions work together to find a common ground regarding the length of time the information is to be retained, as well as who can access and use it. In some cases, de-identification or anonymizing techniques may be employed to allow for longer retention of the record or aggregate data while reducing the risk posed by the sensitive elements.

Additional tactics with an eye to privacy and security should include the following:

Develop a privacy policy and program. A comprehensive privacy policy includes both internal and external-facing versions. Internal privacy policies should include guidelines for handling sensitive information, IT security controls, and breach reporting. External policies are customer-facing and serve to define how the organization manages and protects the information it receives from clients and customers.

As such, external policies have marketing and public relations implications, but it is also important that organizations have the ability to follow through on their external policies. Global policies, both internal and external, require additional attention because of the occasionally conflicting rules of various jurisdictions.

Adopt preventative measures, such as the following:

- Implement a *Data Loss Prevention* system, technology that is designed to detect a potential data breach and to prevent it by monitoring, detecting, and blocking sensitive data. Sensitive data may include private or company information, intellectual property, financial or patient information, credit-card data, and other information depending on the business and the industry.
- Engage in *Data Minimization*, reducing the amount of sensitive data that is retained in the first place, by asking questions such as:
  - Does the organization really need to keep the data? Some data is transitory in nature and may be needed at the moment, but not for the long-term.
  - Can the information be anonymized and still serve the same purpose? For example, if the business wants to track customer activity over a period of time, does it need the full details of each transaction, or would anonymized or aggregated data meet the need?
  - Could less sensitive data be used in place of this data? For example, instead of storing information such as a driver's license number, a customer ID that is only used by the organization may suffice.
- Implement a *Cloud Storage Policy* that defines the data protection and security requirements for data stored with a third party provider of cloud storage.

Develop a comprehensive breach response plan. Although the preventative measures discussed above may help avoid a data breach or cyber attack, an organization is wise to develop a comprehensive breach response plan. In the event a breach should occur, immediately implementing the comprehensive breach response plan may help minimize the impact and damage. Following are some factors to consider including in the response plan:

- Understand the state and federal reporting requirements when a breach occurs.
- Include an immediate assessment of the size and scope of the breach, as well as the location and entry points to determine the source of attack.
- Consider engaging knowledgeable legal counsel and forensic experts to work with law enforcement to supplement the investigation.
- Include an assessment of the damage done, both from a financial and reputation standpoint, and the immediate management of both.
- Because a communication strategy is key, include a formal communication plan and appropriate timing as part of the breach response plan.

E-Discovery

Developing and documenting e-discovery guidelines provides the foundation for demonstrating overall repeatability and defensibility of the organization's discovery processes. Developing standardized e-discovery policies and guidelines provides an organization with the optimized ability to:

- Ensure that the e-discovery process is managed, executed, and documented in a repeatable and defensible manner.
- Establish and communicate roles and responsibilities of attorneys, legal staff, IT, records coordinators, and outside counsel throughout the discovery process.
- Comply with applicable state and federal laws as well as "best practice" guidelines and recommendations pertaining to electronic discovery.
- Reasonably respond to regulatory inquiries, discovery requests, and subpoenas in an efficient, effective, and fiscally responsible way.

An organization should implement documented policies and guidelines for e-discovery-related processes including initial case assessment, legal hold, collection, processing, review, and production, Without defined and documented policies and guidelines, e-discovery process consistency and integrity are potentially vulnerable to the scrutiny of opposing counsel and the courts.

Employee training and compliance

Monitoring and reporting on employee compliance with Information Governance policies and procedures is a critical component of a successful program. A formal compliance review process should include employee training on the Information Governance policies to help them understand their responsibilities and to facilitate their alignment with policy directives, followed by compliance reviews. Training should be provided at the following time points:

- When a new policy is issued or when a significant revision is made,
- During new employee orientation, and
- Annually, in conjunction with the overall ethics and compliance policy review.

Following training, compliance reviews should assess employees' awareness and understanding of the governance policies and their requirements and their acknowledgment of their responsibilities regarding the policies.

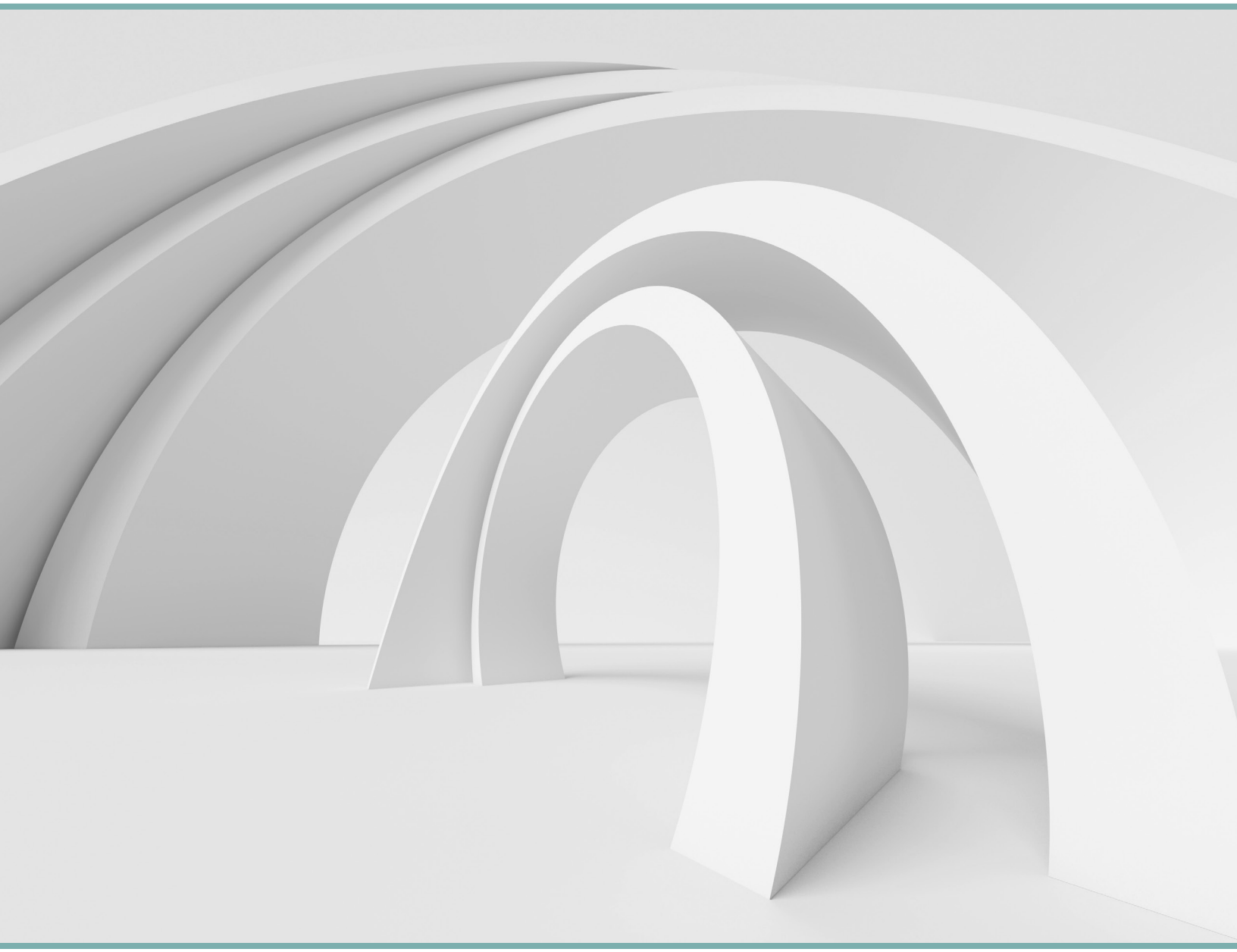
Without defined and documented policies and guidelines, e-discovery process consistency and integrity are potentially vulnerable to the scrutiny of opposing counsel and the courts.

CONCLUSION

The conflicting requirements of diverse stakeholders that affect the lifecycle management of information, from its creation or receipt until its final disposition, can be addressed by a comprehensive Information Governance approach. Reconciling these conflicts will help ensure that all interested stakeholders' needs are not only met, but optimized. Further, holistic Information Governance will allow organizations to leverage information as a key asset, supporting the combined objectives of reducing risk, enhancing compliance, boosting efficiency, and realizing company mission and vision.

Laurie Fischer
Managing Director
lfischer@hbrconsulting.com
312.638.5127

Laurie leads the Information Governance practice tailored to address the increasingly complex and demanding regulatory and technological challenges of today's information management environment. Laurie has over 25 years of consulting experience partnering with clients of all industries and sizes to help them achieve their enterprise-wide compliance and governance objectives.



HBR
CONSULTING

HBR Consulting (www.hbrconsulting.com) delivers advisory, managed services and software solutions that increase productivity and profitability, while mitigating risk for law firms, law departments and corporations. Thought leaders with decades of experience, we deliver value to our clients. HBR has long-term relationships working with 90 percent of Am Law 200 law firms and 35 percent of Fortune 500 corporate law departments.