

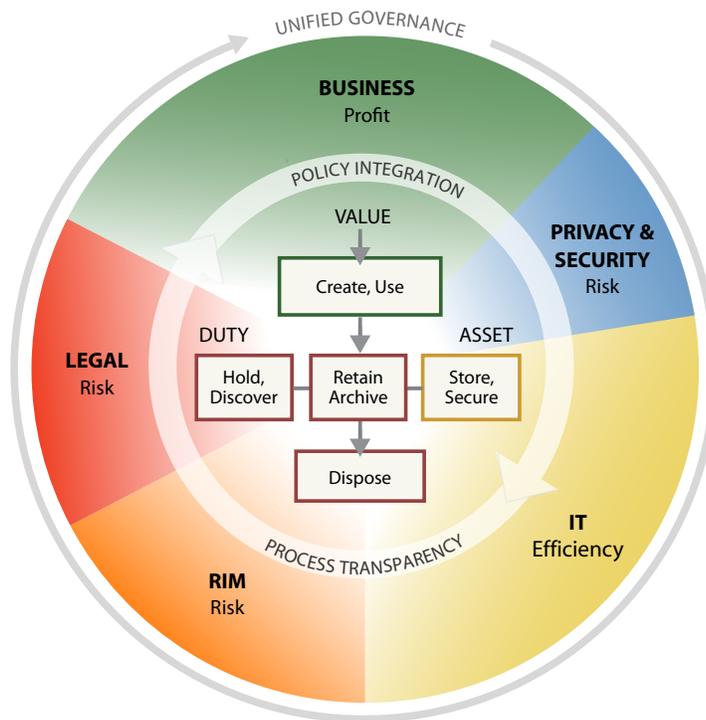
IGRM v3.0 Update: Privacy & Security Officers As Stakeholders



Privacy & Security Added to The Information Governance Reference Model (IGRM) v3.0 to Provide Cohesive Governance Framework for Legal, Records, Privacy, IT and Business Information Stakeholders

Introduction

The Information Governance Reference Model (IGRM), depicted in Figure 1 is a tool for communicating with organizational stakeholders regarding the responsibilities, processes, and practices for information governance. The IGRM illustrates the relationship between key stakeholders and the Information Lifecycle and highlights the transparency required to enable effective governance. The IGRM promotes cross-functional dialogue and collaboration with the goal of achieving higher levels of information governance. It fosters efficient and appropriate data management that enables defensible disposal — by effectively aligning information value to information cost.



Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

Fig 1. Information Governance Reference Model (IGRM) © 2012 v3.0 edrm.net

The purpose of this white paper is to provide corporations, analyst firms, industry associations, and other parties with a stronger understanding of how the IGRM framework facilitates better cooperation among stakeholders, drives cross-functional processes, and aligns information governance goals across the organization. This paper also provides background related to the creation of the IGRM and the relationship to the Electronic Discovery Reference Model (EDRM) community.¹

Framework

The IGRM provides a framework for defining a unified approach to information governance by showing the linkage between value and duty to information assets. The IGRM diagram is a responsibility model rather than a lifecycle model (like EDRM). The IGRM is also not intended to be an organization chart—companies can (and are expected to) organize their various roles and responsibilities in different ways. The specific responsibilities and who represents the various stakeholders will vary from organization-to-organization.

The IGRM brings forth the reality that dependencies exist across the various stakeholder groups and addressing the information risks of one, such as legal compliance or privacy issues, should not be addressed in a vacuum. The IGRM also helps to highlight and define these dependencies and allows for stakeholders to understand their role in information governance and achieve defensible disposal. It also further defines the stakeholders' respective "stake" in information governance, and highlights the intersections and interdependencies across these stakeholders.

The IGRM can serve to establish the importance of linking stakeholders, particularly those responsible for ensuring that the legal duties related to handling information are met, to those that understand the business value of information and, in turn, to those that manage information assets. Accordingly, the IGRM framework may be updated over time to reflect evolving needs, best practices, and thought leadership in information governance focusing on lowering information cost and risk.

¹ Specific key material terms and elements described herein are defined in greater detail in the Glossary of Key IGRM Definitions which are listed at the end of this paper.

Development and Purpose of the IGRM

The IGRM was developed by members of the EDRM with expertise from RIM, Discovery, Legal/Regulatory Compliance, Privacy & Security, and IT. It was a community effort developed over the course of a year. Prior to its initial publication, the diagram was socialized through the membership of both the EDRM and the Compliance, Governance, and Oversight Council (CGOC) with more than 1900 legal, IT, records and information management professionals from corporations and government agencies. Shortly after the publication of the first IGRM, the model was endorsed by ARMA International.²

The impetus for the IGRM came from a joint survey conducted by the IGRM project group of the EDRM and the CGOC³. The results from corporate practitioners showed:

- 100% of respondents stated that defensible disposal was the primary purpose of information governance;
- 66% of IT and 50% of RIM respondents said their current responsibility model for information governance was ineffective; and
- 80% of respondents across Legal, IT, and RIM said they had little or very weak linkage between legal obligations for information/data and records management.
- Optimizing e-Discovery processes using the IGRM is a hot topic for discussion by attorneys, technologists, and executives within prominent organizations.⁴

Elements of the IGRM

The following section describes the core elements of the IGRM.

The Business Value of Information

The business stakeholder is primarily responsible for “Profit”. In this capacity, the stakeholder has an interest in information proportional to its value – the degree to which it helps drive the profit or purpose of the enterprise itself. If that value expires, the business could lose interest in managing it, cleaning it up, or paying for it to be stored. IGRM distinguishes information value from regulatory obligation or IT efficiency. The diagram defines the business group’s responsibility to categorize, define, and declare the specific value of information; all data does not have value and the value of data is not constant.

² How the Information Governance Reference Model (IGRM) Complements ARMA International’s Generally Accepted Recordkeeping Principles (The Principles), available at <https://www.arma.org>

³ 2010 Information Governance Benchmark Report in Global 1000 Companies, available at <https://www.cgoc.com/register/benchmark-survey-information-governance-fortune-1000-companies>

⁴ Better E-Discovery: Unified Governance and the IGRM, available at <http://apps.americanbar.org/litigation/committees/technology/articles/summer2012-0612-e-discovery-unified-governance-igrm.html>

Legal and RIM Have Compliance Responsibilities

Legal and RIM on the left side are chartered typically to manage different factors impacting legal risks and compliance for the company. The diagram underscores that it is the legal department's responsibility to identify what to put on legal hold (i.e., suspend expiry) and what to collect/process for discovery. Likewise, it is RIM's responsibility to ensure that regulatory obligations to retain information for the requisite period and the required format are satisfied. Together they both have an enormous role in how and when companies can dispose of data.

IT is Chartered with Efficient Management

IT has the responsibility to store and secure information under their possession, custody, or control. This stakeholder's primary focus is on increasing efficiency and decreasing costs for managing the information assets. IT is also responsible for facilitating the needs of the business to achieve profit. As the diagram aptly portrays, unified governance is necessary for IT to appreciate the value and understand the duties associated with specific types of information. IT facilitates the creation and maintenance of business value and executes on Legal, RIM, and Privacy & Security's requirements for compliance and risk mitigation – all the while maximizing process efficiency.

Privacy & Security Establish Appropriate Access Restrictions and Controls

Privacy & Security, as stakeholders, were recently added to the IGRM. The first iteration of the model included reference to “store” and “secure” in the Information Lifecycle diagram, but upon further reflection, the members of IGRM felt issues related to privacy and security are significant enough to warrant the addition of a new stakeholder. Privacy & Security stakeholders are responsible for identifying and managing risks associated with personal and/or confidential information. The risks may be legal/regulatory in nature, driven by brand/reputational considerations, or both. With respect to privacy and personal information, companies must be cognizant of laws and “best practices” governing transparency and classification at the point of creation, must understand how the data may be collected, used/processed, and where the data may flow (i.e., cross-border data transfers). Confidential information – be it personal or business proprietary – must be appropriately protected as an asset. Implementation of standards to ensure reasonable and appropriate security protocols - technical, physical, and administrative – is critical for proper information risk management. Enhanced security protocols may be warranted or required for sensitive data (e.g., protected health information, data that could facilitate identity theft, discrimination, or harm, trade secrets, proprietary information, etc.).

The Information Lifecycle Governance

The middle of the diagram calls out specific information concerns in the governance strategy that most closely organize around the nearest stakeholder. Those concerns are shared with other stakeholders through process transparency and policy integration requirements for improved governance and defensible disposal. Starting at the top and moving clockwise, the business is responsible for generating revenue, reducing costs and satisfying customers. Information is created and used to satisfy those concerns. Starting at the point of creation and throughout the lifecycle, organizations have a duty to ensure information is properly handled and personal or confidential information is appropriately protected. Classifying information for easy retrieval results in faster access while Business is using the information, and classification makes it easier to access data needed for discovery and/or investigation. As information exists in storage and in transit, IT is chartered with storing and securing information on behalf of the business and executing on the requirements established by Legal, RIM, and the Privacy & Security stakeholders for compliance. As organizations are governed by the laws and regulations in the jurisdictions in which they operate, RIM brings forth the obligations for information and recordkeeping, including what, how, for how long, where, and in what format information is retained and archived. Once data is created, it is potentially subject to legal hold and discovery as part of investigations, litigation, or other adversarial proceedings. Organizations need access to information to prove their own claims as well as to defend against claims made against them by customers, employees, competitors, law enforcement/regulators or other adversaries. Organizations may also find themselves in possession of third party information that is sought by plaintiffs, defendants, or law enforcement/regulators to support a claim or defense. Legal, as advocates and defenders of the organization, prescribe what and how information is held and discovered in response to requests for data.

The process transparency and policy integration continuum highlights the fact that the proper information governance is not linear and requires input from all stakeholders. For example, Privacy & Security work closely with RIM on retention policies and protocols while Legal instructs IT on holds and collections. IGRM and the underlying governance framework provides flexibility for stakeholders to drive or participate to accommodate their interdependence and mutual interest on the very same information.

The Relationship Between the IGRM and the EDRM

While the well-known EDRM diagram is a process flow model for e-Discovery, the IGRM diagram is a stakeholder model that illustrates the interrelated responsibilities for information governance.

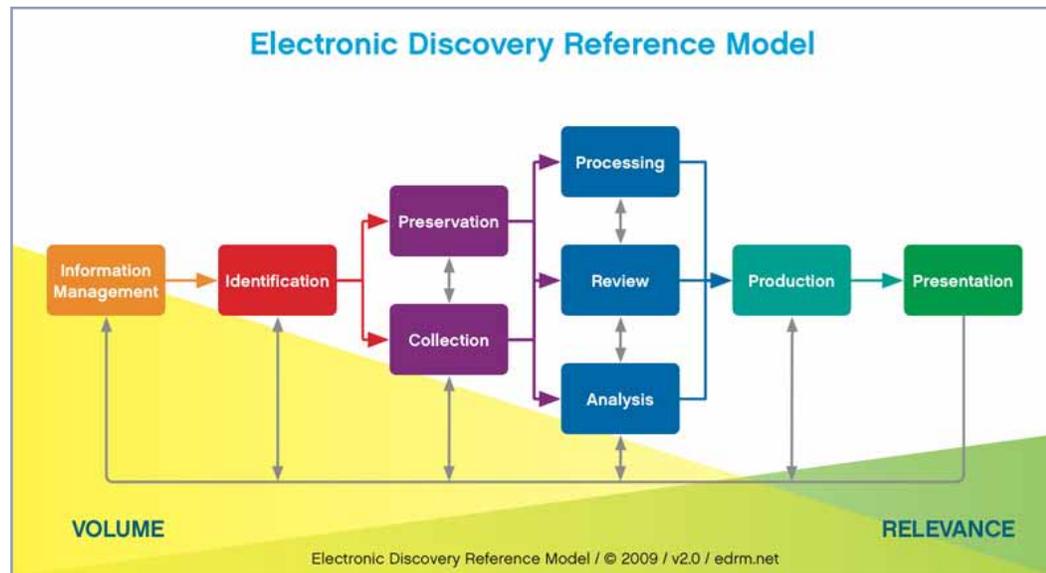


Fig 2. Electronic Discovery Reference Model (EDRM) © 2009 v2.0 edrm.net

To best understand the relationship between the two models, it is important to first acknowledge their differences. Information governance is a broad strategy where a myriad of decisions are made with regard to the creation, use, processing, protection, management, and disposition of information. The IGRM reflects a continuous flow of activity whereby each stakeholder's individual function supports the continual governance of information assets and how information is handled to lower information cost and risk.

The process of e-Discovery is an example of one aspect of information governance. The EDRM represents one aspect of the IGRM strategy. The process of e-Discovery can be viewed as a use case for the IGRM. As a stakeholder model, the IGRM illustrates the collaboration necessary for fulfilling e-Discovery obligations – Business, IT, Legal, RIM, and Privacy & Security need to all work together.

It is important to emphasize that the IGRM is not the first node of the EDRM. The first node of the EDRM is "Information Management" and represents the specific policies and procedures that govern the management of ESI relevant to the process of e-Discovery. The Information Management node helps to illustrate how effective management of ESI can positively impact the entire e-Discovery workflow — by reducing volume, increasing efficiency, and lowering related risks and costs.



The Information Management node of the EDRM can, however, be viewed as a gateway between the process of e-Discovery and the broader strategy of information governance. ESI volume is depicted in the EDRM by a yellow triangle. As you work through the e-discovery process, you should find that an increasingly large percentage of the ESI you are handling is relevant to your project. Generally, the increase in relevance, as depicted by the green triangle, goes hand in hand with the decrease in volume. ESI are processed and analyzed, relevant data are identified depicted by the smaller green triangle. This corresponds with the stakeholders's goal of enabling defensible disposal of information, depicted at the center of the IGRM by the information life cycle. Also, each grey line in the EDRM model points back to Information Management, depicting where disposal takes place and volume reduction occurs. These parallel features between the models further represent that effective information governance will lead to more efficient information processes, e-Discovery included.

Application of the IGRM Diagram

While there are many lifecycle models for information and the EDRM lifecycle model for a legal case, most companies are unable to defensibly dispose of information for lack of transparency across legal, RIM, Privacy & Security, and IT organizations and lack of systematic linkage among their processes.⁵ Detailed lifecycle models that are anchored in a single discipline, such as discovery or records management, often fail to garner the level of senior management attention and support that can galvanize true change and charter the kinds of programs and practices that enable timely, defensible disposal of information. The IGRM can provide the needed executive catalyst and complement the detailed discipline tools that are offered by organizations like ARMA, AIIM, and The Sedona Conference.

Conclusion

Understanding the IGRM diagram and its basic elements is the first step on the path to achieving unified information governance focused on ensuring the duties and value of information are tightly coupled with information assets, enabling defensible disposal and lowering costs and risk.

Today, many key stakeholders and departments could stand to improve how they collaborate and communicate with each other. Fostering cross-functional objectives

is a key aspect of a successful information governance strategy. The IGRM is a tool that reinforces and illustrates the inter-connectivity of people and processes required for effective information governance. By raising awareness internally—and through reinforcement of the IGRM—you can bolster coordinated efforts by core stakeholders to garner full executive support. Achieving unified information governance then becomes feasible with genuine corporate acceptance and commitment.

⁵ IDC projects that data volume will increase by a factor of 44 over the next 10 years and litigation costs and preservation obligations escalate continuously, creating an unworkable situation for many companies.

Glossary of Key IGRM Definitions

Asset

The specific container of information that IT stores and secures under their management. The primary driver is to increase “Efficiency” and lower costs associated with this function.

Duty

Legal obligation for managing the “Risk” associated with specific information. Legal and RIM have the responsibility for legal duties and obligations (i.e., legal hold preservation and regulatory retention obligations)

Information Governance

The specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals (as defined by Gartner).

Information Governance Reference Model (IGRM)

A framework and responsibility model for cross-functional and executive dialogue that serves as a catalyst for defining a unified governance approach to information by linking business value and legal duties to the information assets.

Policy Integration

A formalized common set of goals and rules that promote cross-functional communication, collaboration, and optimization. Information governance efforts can be crippled by failure to integrate policy.

Process Transparency

The shared ownership and execution of Information Governance processes ensuring that accountabilities and dependencies across the stakeholders are clearly defined by each group to promote efficient and effective management of information.

The Generally Accepted Recordkeeping Principles ® (“The Principles”)

The Principles reflect standards and guidelines related to records management, developed by ARMA International, a not-for-profit professional association and a widely-recognized authority on managing records and information. The Principles include: (1) Principle of Accountability, (2) Principle of Integrity, (3) Principle of Protection, (4) Principle of Compliance, (5) Principle of Availability, (6) Principle of Retention, (7) Principle of Disposition, and (8) Principle of Transparency.

Unified Governance

Unified Governance is a marriage between policy integration and process transparency. Effective unified governance creates an organizational environment whereby the key stakeholders have a defined partnership with executive buy-in and oversight to create a uniform approach and to establish a strong linkage between legal obligations for information, records management, and IT; and the duty and value associated with the data asset.

Value

Utility or business purpose of specific information. The line of business has an interest in information proportional to its value—the degree to which it helps drive the “Profit” or purpose of the enterprise itself, its mission and goals.



About ARMA International

ARMA International is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession with a current international membership of nearly 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. It also publishes the award-winning Information Management magazine. The association also develops and publishes standards and guidelines related to records management. It was a key contributor to the international records management standard, ISO-15489. For more information, please visit <http://www.arma.org>.

CGOC

About CGOC (Compliance, Governance and Oversight Council)

CGOC (Compliance, Governance and Oversight Council) is a forum of over 1900 legal, IT, records and information management professionals from corporations and government agencies. CGOC conducts primary research, has dedicated practice groups on challenging topics, and hosts meetings throughout the U.S. and Europe where practice leaders convene to discuss discovery, retention, privacy and governance. Established in 2004, it fills the critical practitioners' gap between EDRM and The Sedona Conference. For more information, please visit <https://www.cgoc.com>.



About EDRM

Launched in May 2005, the EDRM Project was created to address the lack of standards and guidelines in the e-discovery market – a problem identified in the 2003 and 2004 Socha-Gelbmann Electronic Discovery surveys as a major concern for vendors and consumers alike. The completed reference model provides a common, flexible and extensible framework for the development, selection, evaluation and use of e-discovery products and services. Expanding on the base defined with the Reference Model, the EDRM projects now include nine projects including the Information Governance Reference Model project. Over the past seven years, the EDRM project has comprised more than 250 organizations, including 170 service and software providers, 61 law firms, three industry groups and 22 corporations involved with e-discovery. Information about EDRM is available at <http://www.edrm.net>.



© 2012 EDRM

