

# Good Information Governance: Addressing Compliance, eDiscovery, and Information Privacy in the Enterprise

*Best Practices Planning*

---

## **Abstract**

This white paper defines good information governance (“good governance”) as it applies to compliance, eDiscovery, and information privacy. It addresses the challenges in each area. Then it presents a model for a good governance best practices architecture and discusses the components such an architecture includes.

October 2008

---

---

Copyright © 2008 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

**THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on [EMC.com](http://EMC.com)

All other trademarks used herein are the property of their respective owners.

h4596

---

## Table of Contents

<b>Executive summary .....</b>	<b>4</b>
<b>Introduction .....</b>	<b>4</b>
Audience .....	5
<b>What is good information governance? .....</b>	<b>5</b>
Attributes of a good information governance strategy .....	6
<b>Meeting the challenges of good information governance.....</b>	<b>6</b>
Corporate governance and regulatory compliance.....	6
Good information governance enables sustainable compliance .....	7
eDiscovery .....	8
Good information governance supports proactive eDiscovery .....	8
Information privacy.....	9
Good information governance protects information wherever it resides.....	10
<b>Getting started with good information governance.....</b>	<b>10</b>
Integrated content archive .....	11
Retention policy management .....	11
The tools of retention policy .....	12
<b>A best practices architecture for good information governance.....</b>	<b>12</b>
Multiple client access .....	13
Controlled lifecycle enforcement.....	14
Records management.....	14
<b>Use case—life sciences .....</b>	<b>15</b>
<b>Use case—public sector .....</b>	<b>15</b>
<b>Conclusion .....</b>	<b>16</b>

---

## Executive summary

Good information governance (“good governance”) is a proactive, policy-driven information management strategy for the global enterprise. It integrates enterprise business objectives with information management policies that address corporate governance and regulatory compliance, eDiscovery, and privacy mandates holistically throughout the information lifecycle. It standardizes and automates processes and policies across line-of-business (LOB) systems and IT infrastructure.

A good governance strategy should simplify the demands and lessen the inherent difficulties of managing information for regulatory compliance, eDiscovery, and privacy. In all three areas the challenges are similar, but they have different risk profiles and business impacts. The same good governance foundational technologies that address information management challenges in corporate governance and regulatory compliance can also be applied to eDiscovery and information privacy.

A best practices architecture for good information governance ensures the integrity, security, and accessibility of information. Through multiple client access points, it delivers the ability to manage regulated content with automated, enforceable retention policies and an integrated content archive that accommodates content of any type.

EMC has deployed stringent good information governance solutions for hundreds of Global 2000 companies in highly regulated industries such as financial services and life sciences. The core of these solutions, and the foundation of our best practices good governance architecture, is the EMC<sup>®</sup> Documentum<sup>®</sup> content management platform, which is National Information Assurance Partnership Common Criteria (EAL 2) certified.

## Introduction

In 2006, the world created, captured, and replicated more than 150 exabytes of digital information—enough to hold 3 million copies of every book ever written.<sup>1</sup> Between 2006 and 2011, the information added annually to this digital universe will increase to nearly 1,800 exabytes. That’s a compound growth rate of almost 60 percent.<sup>2</sup> These numbers strain the imagination. We can define an exabyte in terms of equivalent petabytes, terabytes, gigabytes, and so forth. But what does it really mean? Well, in simpler terms, one exabyte is the equivalent of 50,000 years of DVD quality video.<sup>3</sup> We create some 20 exabytes of data just by *telephone* every year!<sup>4</sup>

Bret Swanson, senior fellow at the Discovery Institute, calls this rapid expansion of the digital universe “the exaflood.” And, your enterprise sits squarely in its path. Actually, off-the-charts digital data growth has been business as usual for most large enterprises for close to a decade. Business as usual, yes. Under control, no. In fact, industry research estimates that as much as 90 percent of unstructured information—information not in databases—goes unmanaged. Moreover, it is often spread across hundreds of systems and applications, many of which do not allow easy access. It’s no wonder that across the information lifecycle—create, manage, deliver, archive, and retire—as much as 80 percent of IT budgets can be consumed by simply maintaining infrastructure and multiple systems.

---

<sup>1</sup> “The Expanding Digital Universe, A Forecast of Worldwide Information Growth Through 2010”, IDC, March 2007

<sup>2</sup> “The Diverse and Exploding Digital Universe”, IDC, March 2008

<sup>3</sup> Gross, Grant (November 24, 2007). “Internet Could Max Out in 2 Years, Study Says”, *PC World*

<sup>4</sup> Swanson, B (January, 20, 2007). “The Coming Exaflood”, *The Wall Street Journal*, Retrieved July 3, 2008, from <http://online.wsj.com/article/SB116925820512582318.html>

---

Of course, no one denies the value of information. It boosts innovation and helps sustain competitive advantage. Information refreshes the product development pipeline, supports sales and marketing, enriches collaborative efforts with partners, and contributes to more responsive customer service.

Nevertheless, beyond the issues of volume and complexity, information poses serious legal and regulatory risks. First, from the seemingly trivial e-mail message to the most closely guarded intellectual property, it is all subject to eDiscovery, which is an area of growing concern for all large organizations—especially publicly traded companies. In 2007, Fulbright & Jaworski’s Litigation Trends Survey pointed out that 20 percent of the largest companies surveyed had between 21-50 lawsuits with \$20 million or more at stake.<sup>5</sup> Responding to discovery requests and defending against lawsuits put intense pressure on enterprise information management systems—intense and expensive pressure.

Many types of information are also the object of regulatory scrutiny, and companies have regulatory duties with regard to that information. They must protect its privacy and security, make it available for defined time periods, document the processes and approval procedures with which it’s handled, and prove those procedures were followed. In some cases, information must be retained for as long as 30 years or for the lifetime of the individual to whom it pertains. There are stiff penalties for noncompliance and, of course, very public and embarrassing accounts in the press when confidential information disappears or ends up where it shouldn’t.

The greater the volume of information, the more varied the file types, and the more systems on which it resides, the greater the possibility that something important will be lost, misplaced, or simply overlooked. Taken together, these issues create the challenge of good information governance (“good governance”). The remainder of this white paper defines good governance, describes a technology platform that can support it, and explains how good governance delivers measurable benefits in the areas of corporate governance, regulatory compliance, eDiscovery, and information privacy.

## **Audience**

This white paper is intended for a broad audience of IT and information management professionals. It includes CIOs, IT directors and litigation support, storage administrators, compliance officers, information architects, and records managers.

## **What is good information governance?**

Good information governance (“good governance”) is a proactive, policy-driven information management strategy for the global enterprise. Good governance integrates enterprise business objectives with information management policies that address corporate governance and regulatory compliance, eDiscovery, and privacy mandates holistically throughout the information lifecycle. It standardizes and automates processes and policies across line-of-business systems and IT infrastructure.

A good governance strategy enables organizations to deploy flexible information governance solutions that address local and global requirements while:

- Responding quickly to changing compliance demands

---

<sup>5</sup> Fulbright & Jaworski, 2007 Litigation Trends Survey, October 2007

- 
- Reducing eDiscovery costs and risks
  - Demonstrating a commitment to privacy
  - Enhancing the business value of archived content
  - Decreasing the volume of stored content and associated storage costs
  - Delivering a sustainable competitive advantage

### ***Attributes of a good information governance strategy***

A good governance strategy should simplify the demands and lessen the inherent difficulties of managing information for corporate governance, regulatory compliance, eDiscovery, and privacy. To do that, the strategy should be:

- Sufficient, not excessive
- Balanced between risk mitigation and cost containment
- Proactive and enterprisewide
- Repeatable and programmatic
- Adaptable to content and business requirements

The foundation technologies that enable good governance include controlled content lifecycle enforcement, retention policy management, classification, search, integrated content archiving, and other content services.

## **Meeting the challenges of good information governance**

The same good governance foundational technologies that address information management challenges in corporate governance and regulatory compliance can also be applied to eDiscovery and information privacy. In all three areas the challenges are similar, but they have different risk profiles and business impacts. The next three sections examine each area separately.

### ***Corporate governance and regulatory compliance***

Corporate governance concerns internal business practices. Business author Gabrielle O'Donovan defines corporate governance as “an internal system encompassing policies, processes and people, which serve the needs of shareholders and other stakeholders, by directing and controlling management activities with good business savvy, objectivity and integrity. Sound corporate governance is reliant on external marketplace commitment and legislation, plus a healthy board culture which safeguards policies and processes.”<sup>6</sup> Corporate governance touches all lines of business from finance, engineering, and human resources to sales, marketing, and strategic planning. Of course, as O'Donovan's definition suggests, external factors such as legislation affect corporate governance. For example, when the U.S. federal government passed the Sarbanes-Oxley Act in 2002, its intent was to restore public confidence in corporate governance.

Good information governance contributes to the larger goal of good corporate governance. Documenting accounts payable processes and enforcing process rules, managing and auditing a corporate diversity

---

<sup>6</sup> “Corporate governance” (2008, June 25). *Wikipedia, The Free Encyclopedia*, Retrieved 18:53, July 9, 2008, from [http://en.wikipedia.org/w/index.php?title=Corporate\\_governance&oldid=221567852](http://en.wikipedia.org/w/index.php?title=Corporate_governance&oldid=221567852)

---

training program, and revising and distributing standard operating procedures (SOPs) are just three examples of good governance challenges that fall under corporate governance.

Regulatory compliance, on the other hand, involves adhering to and proving adherence to a specification, standard, or law that has been clearly defined. According to Forrester Research vice president Michael Rasmussen, “The U.S. government alone has released 114,000 new regulations since 1981.” Regulatory compliance is also a moving target; regulations are added and changed constantly—to wit the Federal Rules of Civil Procedure (FRCP) rule changes in 2006.

Moreover, there are international regulations such as the UK’s Data Protection Act, the section of the Basel II accords that concerns disclosure, and the EU’s Safe Harbor Privacy Guidelines that apply specifically to digital records. These regulations simply add more complexity to an already difficult regulatory environment. The more complexity, the more potential opportunities to be out of compliance. That’s why, with all the attention that regulatory compliance receives, it’s surprising that according to the AIIM 2006 Compliance Survey nearly two out of three information users still do not understand the compliance risks of information mismanagement.

Often, the line between corporate governance and regulatory compliance is blurry, at least from an information management standpoint. Good governance practices that support corporate governance objectives make regulatory compliance easier as well.

## Good information governance enables sustainable compliance

Sustainable compliance balances risk with cost; it is sufficient but not excessive. Sustainable compliance relies on information policies that are comprehensive, automated, and repeatable. With the number of regulations that the contemporary enterprise faces, it is simply impracticable—not to mention very costly—to address each one individually. In other words, the same policies that enable an organization to meet the provisions of the FRCP, for example, should also be broad enough to support compliance efforts for:

- Sarbanes Oxley
- Gramm-Leach-Bliley
- SEC Rule 17a-3 and 17a-4
- NASD Rules 3010 and 3110
- HIPAA
- FDA 21 CFR Part 11
- FCC Title 47
- And so forth

Retention policy management and an integrated content archive—two key good governance technologies—can ease the administrative burden of compliance-driven and corporate governance record keeping while reducing its cost. Good governance ensures that regulated content resides in a protected repository, governed by retention policies that:

- Preserve information accessibility
- Enforce legal holds
- Prevent changes to or destruction of regulated content
- Provide complete audit trails
- Notify compliance managers as content moves through its lifecycle

---

A good information governance solution for compliance puts the complexities of policy management behind the scenes and out of the hands of business users of information systems. For instance, in a file share environment, administrators can apply retention policies to folders. While completely transparent to the user, any document placed in the folder inherits the folder's retention policy. Similarly, disposition can be handled automatically once content has lived up to its legal obligations or it can be done manually by administrators upon notification.

## **eDiscovery**

As already noted from the Fulbright & Jaworski survey, large organizations spend a lot of money on legal activities. Without a doubt, eDiscovery is one of those activities. eDiscovery is no longer just a niche concern of the corporate general counsel or chief legal officer. The costs and risks of bungled eDiscovery put it high on the priority list of CIOs and CFOs as well. For instance, in 2005 a Florida jury awarded nearly \$1 billion to the plaintiff in a lawsuit against a large, diversified financial services company because the company failed after repeated requests to produce all e-mail relevant to the case. In a nutshell, eDiscovery poses the question, "What information should be kept and for how long?" The answer for many companies has been to keep everything—forever. This, of course, only compounds the problem of search and retrieval, while dramatically increasing the amount of information to be reviewed by outside counsel and the resulting cost to review it.

Whatever weaknesses corporate information systems have are dramatically revealed when they must respond to an eDiscovery request. Complex and disparate systems also add substantial cost and time to the process of searching for and retrieving relevant information. In *Zublake v. UBS Warburg*, the defendant was compelled to produce, at its own expense, e-mails from backup tapes. It was UBS' inability to accurately produce e-mail and other electronically stored information (ESI) in a timely manner that ultimately secured a \$29 million verdict for the plaintiff. For corporations that are juggling multiple cases across jurisdictional boundaries, eDiscovery can quickly overwhelm IT and legal resources and bring entire lines of business to a standstill.

The 2006 rule changes to the FRCP have simply upped the ante in terms of eDiscovery. As a 2007 Forrester study points out, they have forced information managers to ask the question, "Can all electronically stored information potentially relevant to a given litigation matter be found and produced in less than 100 days?"<sup>7</sup> The answer for most, of course, is "No." The study goes on to note that for many legal departments the response to the FRCP has been to enjoin IT to "take care of this."<sup>8</sup> But that is a fool's errand. No IT department can possibly know where all potentially relevant information exists. Relevant to what? And even if it did know, it wouldn't have the necessary legal expertise to handle the information properly. The fact is *potentially* relevant information could be anything, located anywhere.

## **Good information governance supports proactive eDiscovery**

For most companies, eDiscovery is something they react to, not something for which they plan and prepare. In contrast, good governance makes eDiscovery a repeatable business process. It a proactive approach that reduces eDiscovery's risks, costs, and disruptive impact. Proactive eDiscovery relies on automated processes to inventory and classify information and to set policies that govern retention and disposition.

---

<sup>7</sup> Murphy, B. (2007, July, 17). "Abysmal: The State Of Retention Management", *For Information & Knowledge Management Professionals*, Forrester Research, Inc.

<sup>8</sup> Ibid.

---

Policy enforcement creates evidence repositories that generally meet the “reasonable and defensible” criteria courts apply when evaluating information systems and spoliation claims. At the same time, it substantially reduces the risk of inadvertent destruction of documents. When integrated with specialized discovery software, good governance solutions can also cut attorney review time and minimize the inadvertent production of privileged documents.

The outcome of proactive eDiscovery is the ability to quickly and efficiently produce the right set of documents—and no more. It also simplifies compliance with revisions to the FRCP that address ESI.

## ***Information privacy***

Not all information that organizations amass is worth protecting for business purposes or preserving to meet regulatory mandates. A lot of it is digital “junk.” So one of the difficulties organizations face as they struggle to cope with growing information volume is simply keeping track of what’s valuable and what isn’t. It’s the sensitive and confidential information that needs safeguarding. This is information that when shared voluntarily with colleagues, partners, and suppliers is a tremendous asset. It might include:

- Intellectual property such as design specifications, drug formulas, or research
- Contracts and deal documents
- RFP responses
- Price lists
- Executive communications

There is also an evolving relationship between technology and the legal right to, or the public expectation of, privacy in the collection and sharing of personal data. Privacy concerns exist wherever uniquely identifiable personal data is collected and stored, in digital form or otherwise. In the case of customers or employees, it may be information that you need to serve them and that they entrust to you, such as:

- Social Security and account numbers
- Medical histories
- Human resource information

In either case, when information like this is “on the loose,” it becomes a risk and potentially an enormous liability. Three examples involving four well-known companies are illustrative:

- 2008—Two of the world’s largest software companies are involved in a trade secrets dispute in which the defendant is accused of allowing one of its acquired companies to download trade secrets from the plaintiff.
- 2008—An international printing and imaging solutions provider accidentally posted the names, Social Security numbers, addresses, and birth dates of current and former employees to a file-sharing website that was accessed by two unknown parties.
- 2007—A major national retailer revealed that a laptop containing the personal information of approximately 800,000 of its job applicants was stolen from a third-party contractor.

These incidents are not exceptions to the rule; they are the rule. Trade-secret theft is so common that law firm Womble Carlyle maintains a blog (<http://wombletradesecrets.blogspot.com/>) that chronicles trade-

---

secret litigation and pending litigation. Likewise, the continuing saga of data breaches can be followed at The Data Breach Blog (<http://breach.scmagazineblogs.com/>), where it aggregates breaches by the month.

Interestingly, none of the examples feature breaches of external security. External security failures such as denial-of-service attacks and network intrusions are also serious and not uncommon. But, according to a Ponemon Institute (<http://www.ponemon.org/index.html>) survey of 163 Fortune 1000 companies, roughly 70 percent of all reported security breaches were due to insiders.<sup>9</sup> Obviously, firewalls and other perimeter technologies are not enough.

Moreover, as an Enterprise Strategy Group (ESG) report points out, "...a single data breach can result in costly damage control, fines, customer notification, legal expenses and IT remediation: A spokesperson for Providence Health Systems in Portland Oregon claims that a recent data breach will cost the company between \$7 and \$9 million."<sup>10</sup>

## Good information governance protects information wherever it resides

To protect and secure sensitive information, organizations must be able to:

- Control what authorized recipients do with information (copy, paste, edit, forward, screen capture, or print)
- Modify or revoke access rights at any time
- Continuously audit information use

These capabilities cannot be location centric. They must be applicable wherever information resides—within the organization or beyond its firewall. A good information governance solution accomplishes this via information rights management (IRM), also known as enterprise digital rights management (EDRM). Gartner defines EDRM technologies as, "...designed to apply encryption-based protective controls directly to data files. EDRM systems allow enterprises and end users to protect such files, not only on a specific platform, but anywhere a given file may move. The protections are defined and enforced based on the identity of the end user, as well as the policy established for a given class of data or specific file."<sup>11</sup>

IRM can be used to safeguard information that is protected under regulatory statutes such as HIPAA and Gramm-Leach-Bliley. It can help thwart trade-secret theft. And, applied to documents produced during eDiscovery, IRM enables organizations to enforce "digital clawback" agreements that cover inadvertent production of privileged electronic documents.

## Getting started with good information governance

For most organizations, the starting point for good information governance will be the deployment of two key technologies: retention policy management and an integrated content archive. The next two sections

---

<sup>9</sup> Reardon, Marguerite. "Securing Data from the Threat Within", January 11, 2005, [http://news.zdnet.com/2100-1009\\_22-5520016.html](http://news.zdnet.com/2100-1009_22-5520016.html) (accessed August 30, 2007)

<sup>10</sup> Olsik, Jon (2006). "Enterprise Rights Management: A Superior Approach to Confidential Data Security", White Paper, page 5

<sup>11</sup> Wagner, Ray (2007, February 28). "Key Selection Criteria for Enterprise Digital Rights Management Products", Retrieved February 12, 2008, from Gartner website: [www.gartner.com/resources/146700/146714/key\\_selection\\_criteria\\_for\\_e\\_146714.pdf](http://www.gartner.com/resources/146700/146714/key_selection_criteria_for_e_146714.pdf)

---

will discuss these technologies in some detail. They are essential components of a comprehensive best practices architecture for good information governance.

## ***Integrated content archive***

A good governance architecture delivers many benefits that aren't available with standalone archival systems. For example, the compliance officer looks to protect information and ensure that all data types are compliant. This requires an integrated content archive (ICA), which provides the ability to ingest, store, and manage various content types including:

- Reports
- Unstructured data such as text documents, presentations, and rich media
- E-mail
- Structured data from applications and databases
- New content types such as blogs, wikis, and mash-ups

An ICA applies consistent business rules to information that enforce internal policies and meet regulatory demands. It can simplify administration by reducing the proliferation of interfaces for managing archived content. An ICA also streamlines search related to internal audits or eDiscovery. It can identify and provide access to all information related to a specific search. For example, a query related to a customer service audit could return an e-mail, customer transaction history, invoice, financial statement, and recorded service call. An integrated content archive can also:

- Allow content objects to be part of enterprise business processes without losing their "archival identities"
- Leverage content services such as renditioning, version control, and rights management that support multichannel publishing while maintaining archive priorities with workflow and lifecycle management
- Enable secure content sharing and complex retention policies with capabilities that operate behind-the-scenes, transparent to the user

## ***Retention policy management***

Retention policy management is the lynchpin of a good governance architecture. When information has material value, it must be kept and kept track of until it can be destroyed. Retention policies define the specifics of why, when, and for how long. They must apply across all arbitrary boundaries that isolate information within an organization. This is where the need for good governance and the characteristics and capabilities of an organization's information infrastructure meet.

A retention policy puts parameters around information that go beyond simple organization or classification. It eliminates ad hoc retention policy decisions by end users and enables administrators to standardize and control the disposition of information across the enterprise. Retention policies can be integrated with and invoked by controlled content lifecycles. Within a best practices architecture, the authority to apply, manage, and configure retention policies can reside in a single corporate compliance role or be distributed by a line of business, which enables retention policies to reflect differing business requirements.

---

## The tools of retention policy

### Conditions

A condition is an event that defines when a retention policy is invoked for a specific object, such as an I-9 employment verification form. For example, termination could be a condition that invokes a retention policy for an employee's I-9 form. Virtually any event can be used as a condition; chronological milestones are often used or passing from one information lifecycle or business process activity to another. Conditions give content administrators and compliance officers a great degree of flexibility in applying retention policies.

### Authorities

An authority is the justification on which a retention policy is based. It is an objective validation of the policy and may be an internal or industry best practice, a court ruling, or a government regulation. A retention policy may have multiple authorities and must have at least one. Retention policies and their authorities are automatically linked and a policy audit will reveal the authorities for all retention policies.

### Freezes and Holds

A freeze “stops the clock” on a retention policy while a hold prevents the deletion of any content governed by it. Each freeze or hold includes a name, description, owner, and creation date. During an audit, investigation, or pending litigation, a hold can be used to ensure that no relevant documents are expunged. This is particularly important during the discovery phase of litigation, where document requests may be very comprehensive and broad based.

### Notifications

A notification alerts designated roles or individuals when an object governed by a retention policy moves from one phase to another or becomes qualified for deletion.

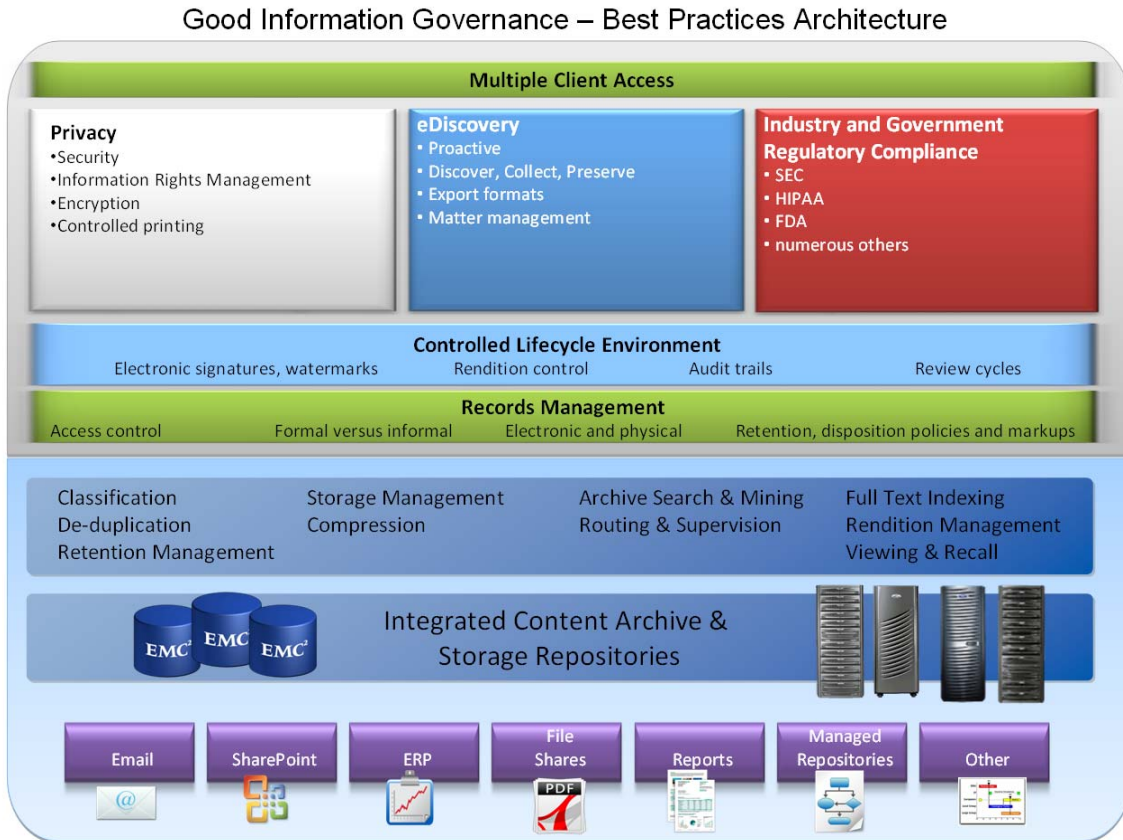
### Audits

All actions associated with a retention policy, including its creation or expiration, changes to configuration, addition or removal of freeze/holds, and who initiated any change, should be auditable.

## A best practices architecture for good information governance

Beyond the fundamentals—retention policy management and an integrated content archive—companies should consider a best practices architecture, which ensures the integrity, security, and accessibility of information. It enables the management of structured, semi-structured, and unstructured content for compliance, legal discovery, storage management, and content reuse. It ensures benefits such as classification, de-duplication, hierarchical storage management, compression, archive search and data mining, routing and supervision, full-text indexing, rendition management, and viewing and recall.

The architecture’s modular components allow these services to be deployed as needed to support existing compliance efforts, launch new initiatives, extend and strengthen enforcement capabilities, and integrate with legacy information systems. This modularity eliminates the need for a costly “rip and replace” approach to improving information governance. A best practices architecture is illustrated in Figure 1.



**Figure 1. The components of a best practices good information governance architecture**

The following sections provide more detail on three key capabilities of a best practices architecture: multiple client access, controlled lifecycle enforcement, and records management.

### ***Multiple client access***

All the rules and processes that a best practices architecture applies and enforces should not make it harder for users to do their jobs. The compliance capabilities, retention policies, and integrated content archive should be easily accessed from virtually any application or desktop, including web-based or portal clients, specialty tools such as eDiscovery applications, and common desktop tools such as those from Adobe and Microsoft. This is the best of both worlds—good information governance that is comprehensive without being invasive.

---

## ***Controlled lifecycle enforcement***

Through controlled lifecycle enforcement, a good governance architecture enables the policy management of information to begin as soon as high-value information is created. A controlled lifecycle consists of policies that are applied and enforced at each state of a document's life. A standard lifecycle could include eight steps: create, review, route, approve, publish, retire, retain, and dispose. But a good governance architecture should allow as many states as needed to map to business processes.

Automated business rules determine what happens as information is promoted or demoted between lifecycle states. For example, as an SOP moves through its review and approval states, security and access control settings may change, files may be moved to a new location or published via a portal, and new renditions may be generated in a variety of file formats. Controlled lifecycle enforcement also ensures that organizations can track chain of custody—determining who has interacted with a particular piece of information, when, and why.

Controlled lifecycles are applicable in a wide range of business contexts. For example, they can be used to:

- Track new drug application (NDA) documents to guarantee proper review, signoff, and submission to the FDA and compliance with 21 CFR Part 11, Electronic Records; Electronic Signatures
- Meet stringent records management requirements by incorporating records management principles and processes
- Ensure that the correct version of information such as SOPs, safety guides, interest rate sheets, and manufacturing specifications is in use

At the same time, controlled lifecycles deliver substantial business benefits including:

- Reduced risk and cost of noncompliance and litigation
- Proven compliance via audit trails
- Increased productivity and faster time to market
- An infrastructure that integrates business functions
- Accelerated content search and retrieval

## ***Records management***

From a legal and regulatory standpoint, anything may be considered a record in so far as it demonstrates compliance with an industry or government regulation or an internal corporate guideline. So, the records management component of a good governance architecture must identify records that should be kept, retain them for as long as required, and dispose of them once they have satisfied their regulatory obligations or corporate governance requirements.

Since records management is such serious business, a good governance architecture that is up to the task must be comprehensive yet flexible. That means it must be able to handle the strict requirements of formal records management that is compliant with standards such as DoD 5015.2 while supporting the management of informal records, which call for baseline retention and disposition policies. Technology that simplifies life for a dedicated records administrator simply adds burdensome complexity for ordinary office workers and managers.

The records management component of a good governance architecture can integrate with an organization's existing records management infrastructure without duplicating storage resources, access controls, metadata management, and administrative tools. Using federation, it permits records management policies to be maintained centrally but applied to information wherever it resides—effectively managing

---

content “in place.” It also delivers the five components necessary for effective enterprise records management:

- Common classification model
- Consolidated search
- Auditing and unified reporting
- Universal retention policy application and enforcement
- Managed disposition

Effective records management in the digital world, where ESI may have to be retained anywhere from months to decades, can impose a mountainous burden on IT departments whose responsibility it is to collect, hold on to, and provide access to that information. In terms of records management, the goal of a good information governance architecture is to reduce that burden—automating the identification of what must be kept, retaining it for as long as necessary, and disposing of it when appropriate to do so in an audited manner.

## Use case—life sciences

All life sciences companies are under pressure to maximize product revenue and shrink development cycle time while meeting FDA requirements. But that requires a streamlined new drug application (NDA) submission process that ensures accuracy and compliance. A typical NDA submission is nearly 1 million pages, including summary and clinical study reports.

Using controlled content lifecycles, a good governance solution can securely and efficiently manage the flow of NDA-related content, enable accurate versioning, authorize and verify recipients, and track changes for electronic submission to the FDA, in compliance with 21 CFR Part 11. It can ensure that all content is produced in a compliant manner and that each document in a submission is the correct document. In addition, leveraging a best practices architecture, good information governance can:

- Provide flexible authoring and collaboration early in the content lifecycle
- Control and audit review, approval, publishing, retention, and disposition
- Prove chain of custody to auditors, investigators, and attorneys
- Increase productivity by automating manual processes

## Use case—public sector

Few organizations or industries have more information to manage than the various branches of federal, state, and local government—or more rules about how it is accessed, managed, exchanged, and published. Like many large corporations, government agencies are struggling to gain a tight rein on this information.

For example, most government agencies deal with hundreds or even thousands of contracts every year. A good governance solution for contracts management can support an automated, paperless system that establishes a standardized, enforceable workflow for contract drafting, review, and approval. Good information governance can ensure compliance with procurement guidelines and prove compliance with comprehensive audit trails. In addition, good governance can:

- Expedite contract approval
- Apply role-based security to the approval process
- Protect contract integrity via information rights management

- 
- Eliminate the physical distribution of contracts between offices
  - Reduce printing and mailing costs
  - Deliver anytime access to contract information

## Conclusion

EMC has deployed good information governance solutions for hundreds of Global 2000 companies in highly regulated industries such as financial services and life sciences. Our experience and market leadership are recognized by analysts and customers alike. The core of these solutions, and the foundation of our best practices good governance architecture, is the EMC Documentum content management platform, which is National Information Assurance Partnership Common Criteria (EAL 2) certified. Employing a unified content platform enables the management of all content types across an organization. When it comes to good governance, this is essential because you can't control what you don't manage. To learn more about good information governance solutions from EMC, visit [www.EMC.com/goodinformationgovernance](http://www.EMC.com/goodinformationgovernance).