



A 15-minute Guide to Enterprise Compliance

Why regulatory compliance is not enough



Foreword

As a business professional, you know time is a precious commodity. You spend much of your day distilling concepts, evaluating options, and managing complex transactions. When you need information, you need it in a form that can be assimilated quickly—forget the mind-numbing detail and get to the point.

With that in mind, we've developed our series of 15-minute guides to essential topics in information management. This guide examines enterprise compliance but from a different perspective than you might expect. While acknowledging that adherence to government regulations is an important part of compliance, it emphasizes two other areas that carry significant risks if ignored but that receive much less attention—information protection and security and eDiscovery and litigation preparedness.

In about 15 minutes, we'll describe three categories of compliance and give an overview of each, explain the risks of focusing solely on regulatory issues, suggest the required capabilities of an end-to-end compliance infrastructure, and briefly touch on the ways in which EMC delivers those capabilities. We think you'll agree that it's 15 minutes well spent.

Table of Contents

<i>Introduction</i>	4
<i>Information protection and security</i>	5
Protecting information wherever it resides	6
<i>eDiscovery and litigation preparedness</i>	6
eDiscovery—the elephant in the room	6
Compliant information management enables proactive eDiscovery	6
<i>Regulatory compliance</i>	7
Corporate governance—the internal side of regulatory compliance	7
<i>The benefits of a compliance infrastructure</i>	8
<i>EMC Documentum compliance infrastructure</i>	8
Content services	8
Compliance services	9
Streamlined user access	9
<i>Learn more</i>	9



Introduction

No one in business would deny that information is a source of innovation and competitive advantage. It refreshes the product development pipeline, supports sales and marketing, enriches collaborative efforts with partners, and contributes to more responsive customer service.

However, at the same time, information is a potent source of legal and regulatory risk. First, from the seemingly trivial e-mail message to the most closely guarded intellectual property, it is all subject to e-discovery, which is becoming an area of growing concern for all large organizations—especially publicly traded companies. In 2005, Fulbright & Jaworski's Litigation Trends Survey pointed out that, "The average \$1 billion-per-year company faces more than 140 cases in the US at one time." This includes lawsuits, regulatory proceedings, and arbitrations.

Putting a precise figure on the cost of all this activity is difficult, but it's not uncommon for a \$1 billion dollar business to spend five percent of its gross annual revenues on legal affairs. That's \$50 million.¹ 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 regards 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. There are stiff penalties for non compliance and, of course, very public and embarrassing accounts in the press when confidential information disappears or ends up where it shouldn't.

Taken together, these issues create the challenge of compliant information management. This challenge is only compounded by the sheer volume and growing complexity of what must be managed—terabytes of structured and unstructured information in a practically endless variety of formats. In fact, industry research estimates that as much as 90 percent of unstructured information goes unmanaged. A recent Enterprise Strategy Group (ESG) report predicts that total worldwide archived digital data in the commercial and government sectors will exceed 27,000 petabytes—or 27 exabytes—in the year 2010.² The greater the volume of information the greater the possibility that something will be lost, misplaced, or simply overlooked.

Finally, this information volume and complexity are mirrored in the IT infrastructure necessary to support them. Information is often spread across hundreds of systems and applications, many of which do not allow easy access. 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.

Understandably, organizations focus on compliance where the perceived need is the greatest—regulatory compliance. After all, there are tens of thousands of regulations worldwide that influence the way in which information is managed. It's a simple crime and punishment equation. Follow the rules—and be able to prove that you followed them—or else. Nevertheless, there are two other areas of compliance that should be of equal concern:

- Information security and protection
- eDiscovery and litigation preparedness

The risks and consequences in these two categories are every bit as prohibitive as those in regulatory compliance.

¹ Fulbright & Jaworski, 2005 Litigation Trends Survey, October 2005.

² Digital Archiving: End-User Survey & Market Forecast 2006-2010, Enterprise Strategy Group, ©January 2006

Information protection and security

Not all information that organizations amass is worth protecting. 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. Without that capability, information that can legitimately be destroyed—and should be, but isn’t—often ends up causing harm.

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:

- Design specifications, drug formulas, or research
- Contracts and deal documents
- RFP responses
- Price lists
- Executive communications

Or in the case of customers and employees, it may be information that you need to serve them and that they entrust to you, such as:

- Social Security numbers
- Medical histories
- Human resource information

When information like this is “on the loose,” it becomes a risk and potentially an enormous liability. Examples from three well-known, national companies are illustrative:

- 2001—A leading healthcare systems company sees its stock plummet 30 percent in one day after a confidential e-mail from its CEO is posted on the Internet.
- 2005—A major financial services institution loses computer data tapes containing Social Security numbers and account information for up to 1.2 million federal employees.
- 2006—An aerospace company reports theft of a laptop containing personal information for over 300,000 past or present employees. The laptop contains Social Security numbers and, in most cases, a home address, phone number, and birth date.

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.

Interestingly, none of the examples feature breaches of external security. External breaches 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.³ Obviously, firewalls and other perimeter technology are not enough.

³ Reardon, Marguerite. “Securing Data from the Threat Within.” January 11, 2005. http://news.zdnet.com/2100-1009_22-5520016.html (accessed August 30, 2007).

Protecting information wherever it resides

To protect and secure information, a compliance infrastructure must be able to:

- Control what authorized recipients may do with information (copy, paste, edit, forward, screen capture, or print)
- Allow access rights to be changed or revoked at any time
- Provide a continuous audit trail that tracks use and demonstrates compliance

But these capabilities cannot be location centric. They must be applicable wherever information resides—within an organization or beyond its firewall.

eDiscovery and litigation preparedness

As already noted from the Fulbright & Jaworski survey, large organizations spend a lot of money on legal activity. That's why the ability to avoid law suits if possible, or respond quickly and effectively when it's not, is one of the major drivers of compliance solutions behind regulatory concerns.

eDiscovery—the elephant in the room

Without doubt, eDiscovery is the elephant in the room that can't be ignored. It's no longer just a niche concern of the corporate general counsel (GC) or chief legal officer (CLO). The costs and risks of bungled eDiscovery put it high on the priority list of chief information officers (CIOs) and chief financial officers (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 (LOBs) to a standstill.

Compliant information management enables proactive eDiscovery

For most companies, eDiscovery is something they react to not something for which they plan and prepare. In contrast, compliant information management enables a proactive approach to eDiscovery that reduces its 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.

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, automated compliance solutions can also cut

attorney review time and minimize inadvertent production such as producing a document that should remain privileged.

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 Federal Rules of Civil Procedure (FRCP) that address ESI.

Regulatory compliance

According to Forrester Research vice president Michael Rasmussen, "The U.S. government alone has released 114,000 new regulations since 1981. So it's little wonder that regulatory issues are the "squeaky wheel" that gets the compliance "oil." Regulatory compliance is also a moving target; regulations are added and changed constantly—to wit the 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 European Commission's proposed MoReq2 that applies 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 AIIIM 2006 Compliance Survey nearly two out of three information users still do not understand the risks of information mismanagement.

Corporate governance—the internal side of regulatory compliance

Although regulatory compliance is primarily thought of in external terms, some of the most important "compliance" issues are those that deal with internal business practices. This is the realm of corporate governance and it touches all lines of business (LOBs) from finance, engineering, and human resources to sales, marketing, and strategic planning. Documenting accounts payable processes and enforcing process rules, managing and auditing a corporate diversity training program, and revising and distributing standard operating procedures (SOPs) are just three examples of information management challenges that fall under corporate governance. Often, the line between regulatory compliance and corporate governance is blurry, at least from an information management standpoint. Good corporate governance makes regulatory compliance easier.

Corporate governance and regulatory compliance demand information management capabilities that:

- Preserve integrity
- Ensure security
- Control accessibility

These same capabilities can also be leveraged to secure proprietary information and meet the demands of litigation.

The benefits of a compliance infrastructure

Because there is so much information to manage, so many rules that apply to that information, and the consequences of mismanagement so dire, compliant information management strategies and tools must make the compliance task easier. Otherwise, it won't be done effectively—or done at all. A compliance infrastructure does this. It makes compliance easier and, in so doing, it also:

- **Mitigates risk**—A compliance infrastructure helps organizations avoid financial and legal sanctions for failure to manage their sensitive information properly or to retain information that might be pertinent to a litigation or regulatory inquiry. (*Zublake v UBS Warburg*, etc.) It not only enables the enforcement of policies and procedures but can provide proof of enforcement as well.
- **Boosts efficiency and reduces costs**—A compliance infrastructure delivers greater control over information. For example, an organization that knows where information resides and what it contains can respond quickly and accurately to eDiscovery requests. By collecting and reviewing only what's relevant, it saves time and money, and may avoid producing privileged information.
- **Improves adherence to regulations and corporate policies**—A compliance infrastructure uses repeatable and auditable processes to preserve the integrity, ensure the security, and control the access to information. These auditable processes enforce and prove adherence to regulatory and corporate governance policies.

An EMC compliance infrastructure

EMC has deployed stringent compliance solutions for hundreds of Global 2000 companies in highly regulated industries such as financial services and life sciences. Our experience and market leadership is recognized by analysts and customers alike. The core of these solutions, and the foundation of our unified enterprise compliance infrastructure, 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 compliance, this is essential because you can't control what you don't manage.

Content services

An EMC compliance infrastructure provides a rich set of content services that can be applied to all content, regardless of type. These services include basic capabilities such as versioning, workflow, and rendition management. But they also encompass more advanced functions such as archiving, unified desktop and enterprise search, auto classification, and more.

The compliance infrastructure's process design and optimization features permit business processes to support regulatory and corporate governance policies and embed rules that assist enforcement.

Compliance services

Compliance services add another layer of information protection, security, and control. For example, controlled lifecycle enforcement can apply policy management to regulated content at every stage, from creation to disposition. Auditing services can prove compliance as well as capture information for business analysis and best practice implementation. Records management and retention policy services ensure that pertinent information is classified and retained with the appropriate level of procedural controls, from simple retention to DOD 5015.2 certified deployments. Archiving enables the capture, policy-based retention, and automatic migration of structured, semi-structured, and unstructured content for compliance, legal discovery, storage management, or content reuse.

Information rights management (IRM) protects information beyond the content repository, wherever it resides. IRM can be used to safeguard information that is protected under regulatory statutes such as the Health Insurance Portability and Accountability Act (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.

An EMC compliance infrastructure provides other capabilities as well, including:

- Encryption
- Access control
- Digital shredding
- SAFE credentialing
- Electronic signatures

The infrastructure’s modular architecture allows 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.

Streamlined user access

All the rules and processes that a compliance infrastructure applies and enforces should not make it harder for users to do their jobs. With an EMC compliance infrastructure, the content repository, content services, and compliance services can be easily accessed from virtually any application or desktop client including enterprise business applications such as Oracle and SAP and common desktop tools such as those from Adobe and Microsoft. This is the best of both worlds—a compliance infrastructure that is pervasive without being invasive.

Learn more

An enterprise compliance infrastructure delivers information integrity, security, and accessibility. It enables organizations to enforce compliance through automated business rules, respond quickly to regulatory inquiries and eDiscovery requests, reduce the cost and complexity of compliant information management, and much more.



About EMC

EMC Corporation (NYSE: EMC) is the world's leading developer and provider of information infrastructure technology and solutions that enable organizations of all sizes to transform the way they compete and create value from their information. Information about EMC's products and services can be found at www.EMC.com.

To learn more about enterprise compliance and the capabilities of an EMC enterprise compliance infrastructure, visit www.EMC.com or call 800.607.9546 (outside the U.S.: +1.925.600.5802).



EMC Corporation
Hopkinton
Massachusetts
01748-9103

1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

EMC, EMC, and where information lives are registered trademarks of EMC Corporation. Documentum is a registered trademark of EMC Corporation. All other trademarks used herein are the property of their respective owners.

© Copyright 2007 EMC Corporation.
All rights reserved. Produced in the USA. 10/07

H3470