

Getting outside help

There's no shortage of records management and storage companies offering compliance-related services. If your company is considering working with such a vendor, McDaniel suggests looking for one that can provide, at minimum:

- Tools, resources and services to help your company develop, maintain and implement effective, organization-wide retention and compliance policies, procedures and training.
- The ability to capture, index, securely store, archive, and retrieve both paper and electronic documents (including email and instant messaging).
- Scalable, flexible services that match your business needs and practices.
- Reports and auditing tools to track and manage inventory and records management programs.
- A transactional system that provides convenient access to search and place orders.
- Timely on-site or off-site destruction that protects confidential information by using modern shredding equipment, highly secure processes and certification of destruction to create a legal audit trail.

In conclusion...

Regulatory compliance continues to grow as a key element of corporate governance. The complexities of compliance, as well as the potential for litigation, make formal records and retention management programs a necessity.

In civil litigation and government investigations, time is an important issue — especially pre-trial. A lengthy discovery process consumes valuable employee time and escalates legal fees, negatively affecting a company's bottom line. Moreover, inefficient processes make it difficult to prove the integrity of business records and may force a company to settle lawsuits based on estimated costs, instead of the merits of the case. While compliance affects the operation of an organization's business, noncompliance can be even more costly due to fines, sanctions, forced case settlements or even imprisonment of company officers.

Comac, an innovator in fulfillment solutions for more than 37 years, is a wholly owned Iron Mountain Company. Iron Mountain Incorporated (NYSE:IRM) helps organizations around the world reduce the costs and risks associated with information protection and storage. The company offers comprehensive records management, data protection, and information destruction solutions along with the expertise and experience to address complex information challenges such as rising storage costs, litigation, regulatory compliance and disaster recovery. Founded in 1951, Iron Mountain is a trusted partner to more than 100,000 corporate clients throughout North America, Europe, Latin America and the Pacific Rim.

For more information, call 1-866-COMAC4U or visit our website at www.comac.com.

This issue of InfoTrak is based on information contained in an article titled "Six stages to reduce costs, risks and complexity of compliance," by Laura McDaniel, Director of the Compliant Records Management Program for Iron Mountain. This article was originally published in *KMWorld*, October 1, 2006.



Corporate Headquarters:
Comac, Inc.
565 Sinclair Frontage Road
Milpitas, CA 95035
1-866-COMAC4U
www.comac.com



InfoTrak

Information for Better Decisions

Can Your Company Meet the Compliance Challenge?

Government regulations — especially those enacted in the wake of accounting fraud and corporate governance scandals — place corporate executives squarely in the hot seat. Failure to fully comply with regulatory requirements can result in:

- SEC sanctions,
- Criminal prosecution,
- Stringent fines,
- Shareholder and customer lawsuits,
- Declining share prices,
- Negative publicity, and
- Loss of public confidence, customer base and market share.

As Laura McDaniel, Director of the Compliant Records Management Program for Iron Mountain sums it up, "Regulatory compliance is an absolute necessity in today's business environment. With growing numbers of regulations from the local, state, federal and industry levels... it has never been more important to keep your organizational house in order."

The regulatory maze

There's no denying that companies operate in an increasingly demanding regulatory environment. In the United States alone, there are more than 10,000 statutes governing their actions.

Provisions focus on three key areas:

- *Governance* — the existence of controls to guarantee that corporate reporting is accurate, timely and complete; retention of corporate records, and disaster recovery and business continuity measures.
- *Privacy* — what personal information can be gathered and kept; how it must be handled (including who, if anyone, it may be given to), and what the company must do if privacy restrictions are breached.

- **Security** — how access to sensitive resources is controlled; how users are identified, and how their access is tracked and audited.

Some regulations cut across industries. For example, the Sarbanes-Oxley Act (SOX) — enacted several years ago in the wake of massive investor losses due to corporate mismanagement — applies to all companies publicly traded on U.S. stock exchanges. SOX's provisions aim to prevent such mismanagement by requiring executives to document and certify internal controls and procedures for financial reporting, to have an external auditor examine financial records, and to maintain audit and review-related information.

Other regulations affect only specific industries or types of businesses. Two well known examples are:

- The Health Insurance Portability and Accountability Act (HIPAA), which focuses on protecting individual health information, specifies not only which data must be protected and stored, but also *how* data must be stored and destroyed to protect privileged information. Its regulations apply, not just to health care providers, but also to companies to which they subcontract functions involving protected data.
- The Gramm-Leach-Bliley Act, which aims to protect the privacy and security of individual financial information that is collected, held, and processed by financial institutions. The privacy provisions require financial institutions to give their customers annual notice of their privacy practices and allow them to opt out of information-sharing arrangements. The safeguards component requires comprehensive security programs to protect the confidentiality and integrity of financial information in their records.

Additionally, there are regulations governing specific activities or business functions, such as the Employment Retirement and Income Security Act (ERISA). ERISA dictates recordkeeping and other requirements for companies offering pensions, 401(k) or other “qualified” retirement plans.

It's also important to be aware of differing jurisdictional regulations and geographic compliance issues. For example, the Sarbanes-Oxley Act has counterparts in Japan (J-SOX), Europe (EU-SOX) and Canada (Rule 198). Here in the U.S., states may add yet another layer of complexity to compliance, such as California's Security Information Breach Notice Act.

Keys to effective compliance

Every regulation is complex in and of itself. But navigating the compliance maze is further complicated by the fact that most companies must adhere to multiple regulations — each of which may have a completely different purpose and scope. This makes compliance not only demanding, but costly, as well.

Companies often adopt reactive, piecemeal approaches in which multiple departments and individuals assume responsibility for the components pertaining to their operations. In its 2006 *Compliance Progress Survey*, ControlPath, a compliance IT company, found that only 30% of respondents have a unified process addressing multiple regulations.

Treating compliance, not as a holistic business issue, but as a fragmented, departmental process, opens the door to errors and omissions or even outright criminal activity. It also increases costs through redundant functions and processes.

In contrast, according to Iron Mountain's McDaniel, a properly designed, enterprise-wide records management program helps ensure that an organization is compliant with all relevant regulations and supports proactive management of discovery requests, thereby controlling litigation risks and costs. Additionally, such programs allow companies to leverage their company's information assets for operational efficiencies that lead to competitive advantage. As a result, she says, “Both costs and risks are reduced, while providing much greater control and access to information.”

Six stages to better corporate governance

Based on her company's experience, McDaniel recommends the following six-stage framework to successfully meet the compliance challenge:

Stage one: organize to create a records management infrastructure.

- Determine your program scope.
- Gain executive-level commitment.
- Establish a steering committee.

Stage two: assess your current program.

- Evaluate your current program status.
- Use risk assessment tools to benchmark against industry peers.
- Identify your most substantial gaps and greatest risks.
- Create a master plan to address and close these gaps.

Stage three: develop key program components and metrics.

- Create one universal records retention schedule that captures all of the records regardless of media.
- Document policies and procedures.
- Define audit metrics to measure the effectiveness of your program.

Stage four: implement your program.

- Implement a base program first.
- Design and roll out training that is tailored for specific audiences.
- Implement technology to assist with program management.

Stage five: monitor and enforce your program.

- Enforce classification and destruction review with online monitoring tools.
- Maintain training, communications and certification programs.
- Update retention schedule, policies and procedures regularly.

Stage six: perform regular audits of your program.

- Incorporate compliance audits into your internal audit function.
- Benchmark findings against your audit metrics and other companies in your industry.
- Recommend improvements and implement corrective actions.

Compliance as a marketing issue

Although compliance is not generally among a Marketing Communications professional's top responsibilities, noncompliance does have implications for marketing. In addition to direct financial costs, the potential damage to a company's brand can be enormous. For example, a study by the Ponemon Institute, which conducts privacy and information management research, reported that about 60% of customers of companies that experience a data breach leave or think about leaving that company.

A company's brand is a valuable asset. Studies show that a strong brand identity encourages customers to buy more, pay more and recommend the brand to their friends. So maintaining brand integrity and consistency is critical. For this reason, marketing personnel should be included in implementing an enterprise-wide compliance strategy.

Marketing should also be vigilant in ensuring compliance with their company's internal requirements, such as brand messaging and design standards, and take steps to give customers and prospects only timely, accurate information. This helps prevent guerilla marketing tactics by dealers, as well as accusations of bait-and-switch by customers.

Your fulfillment company should be a valuable strategic partner in this effort. As a critical link in your marketing chain, a good fulfillment company helps make your communications more effective and efficient. The best companies also offer tools and provide safeguards to keep your communications compliant — both with external legal and regulatory requirements and internal brand, identity and content standards.