



Information Lifecycle Management

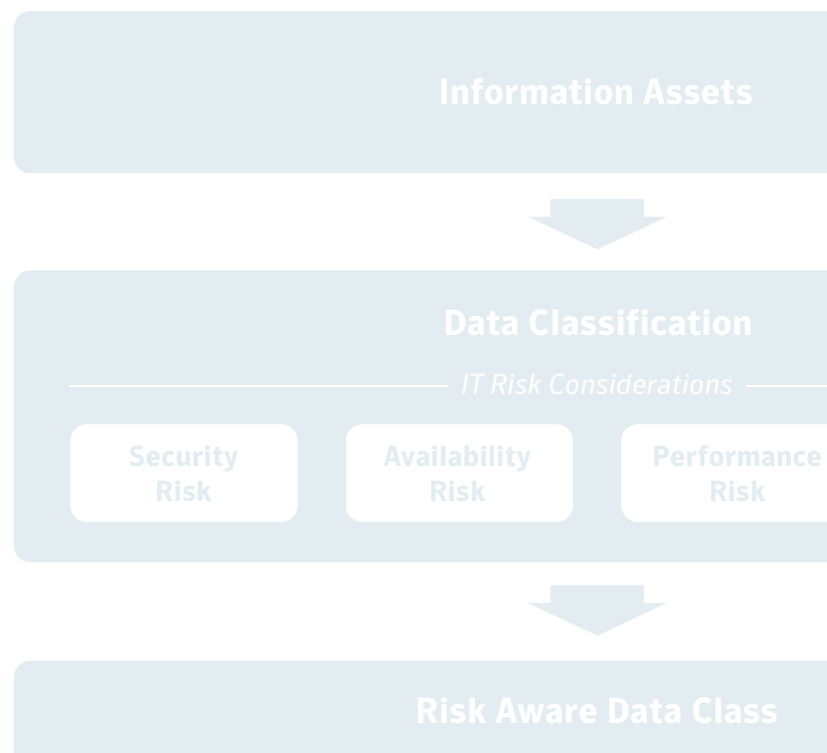
An IT Risk Management Mitigation Report

Volume 1

Executive Summary

IT Risk Management (ITRM) aligns an organization's efforts to mitigate IT security, availability, performance, and compliance risk to its strategic and budget goals. Information Lifecycle Management is both a key technology control within ITRM and an established IT discipline in its own right. By deploying ILM within the framework of IT Risk Management, organizations classify, place, and protect information assets according to their risk-adjusted business value, deploy controls effectively, and avoid unnecessary costs.

Although organizations rate their current ILM efforts as generally effective, supporting and related controls often fall short. This may indicate fragmentation in ILM initiatives that organizations may overcome by deploying ILM within the framework of effective IT Risk Management.



Introduction

Organizations use IT Risk Management to identify and mitigate their IT Risk, including security, availability, performance, and compliance elements. IT Risk managers mitigate these risks by deploying and monitoring process and technology controls – how effectively they do so determines the IT Risk levels their organizations face.

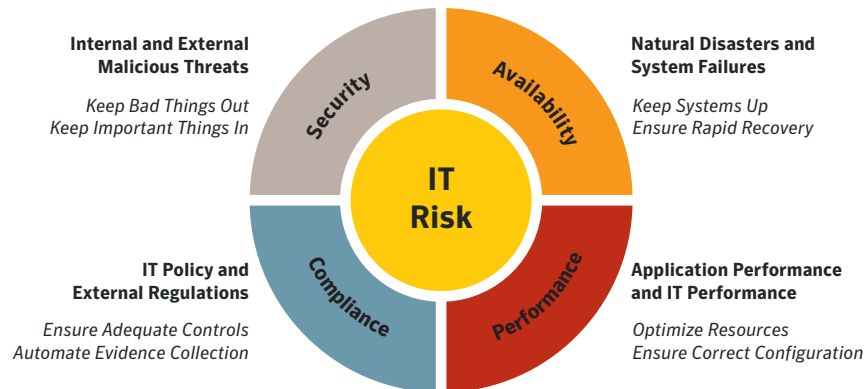


Figure 1: IT Risk encompasses four key elements, each with its own set of drivers and potential business impacts.

Information Lifecycle Management (ILM) is a technology control by which managers classify, place, protect, and archive information, track metadata, and optimize storage. With a long history that predates the emergence of IT Risk Management, ILM is an established IT discipline in its own right. In this paper, we make the case for linking these two powerful disciplines. We examine the intersection between Information Lifecycle Management and IT Risk Management to illustrate both the contributions ILM can make to the management of IT Risk, and how the powerful conceptual framework of IT Risk Management can guide effective implementation of Information Lifecycle Management.

Information Lifecycle Management

Information Lifecycle Management goes by many names, among them Data Lifecycle Management; it is related to storage management, data protection and archiving. Here, we will use definition of ILM from the Storage Networking Industry Association (SNIA):

“The policies, processes, practices, services and tools used to align the business value of information with the most appropriate and cost-effective infrastructure from the time information is created through its final disposition. Information is aligned with business requirements through management policies and service levels associated with applications, metadata, and data.”¹

ILM is not a purchased product or service. Like IT Risk Management, it is something an organization creates for itself. Both disciplines combine people, processes, and technologies, linked to the business value of information and focused on organizational risks and costs. The most effective organizations recognize that these disciplines intersect, and apply them in a complementary fashion.

ILM helps manage IT Risk

IT Risk Management requires understanding and management of information according to its value. Protection of valuable information such as customer records, purchase documents, payroll tables, sales transactions and the like may justify powerful data-protection technologies, with their associated costs, to avoid significant business risks. On the other hand, less-valuable information such as internal newsletters, legacy documentation, instant-messaging archives and media files may require less elaborate and costly technologies to protect it.

The value of information varies according to age as well as type – in fact, this is the origin of the phrase, “Information Lifecycle Management.” For example, protection of up-to-the-minute transaction data may justify expensive high-performance mirroring technologies, while static legacy information presents an opportunity to save on storage costs.

By assigning different values to information assets, organizations avoid the twin hazards of overinvestment in controls to protect lower-value information and underinvestment that leaves critical information at risk. Classifying information by value and deploying controls accordingly, ILM processes help align the actions of IT with the business value of information. Once they are aligned, ITRM guides the planning and design of IT services along with other processes such as data protection, archiving and asset management to support the strategic goals of parent organization.

The intersection of ILM and IT Risk Management

Information Lifecycle Management starts by categorizing an organization’s information assets according to their business value – a process called data classification. This allows IT organizations to deploy people, processes, and technology to provide appropriate levels of security, availability, and performance to each class.

Data classification therefore gives organizations an opportunity to uncover and maximize business value through IT services. For example, if data classification identifies email archives as a source of legal and regulatory risk, IT may implement encryption, searchable disk-based archives, or other processes to reduce exposure. Using the categories of IT Risk to classify information supports fine-grained analysis of the IT Risk associated with individual classes of information, and helps optimize processes to mitigate risks by class. Organizations should identify and mitigate risk at the data-class level as a core good practice for both Information Lifecycle Management and IT Risk Management.

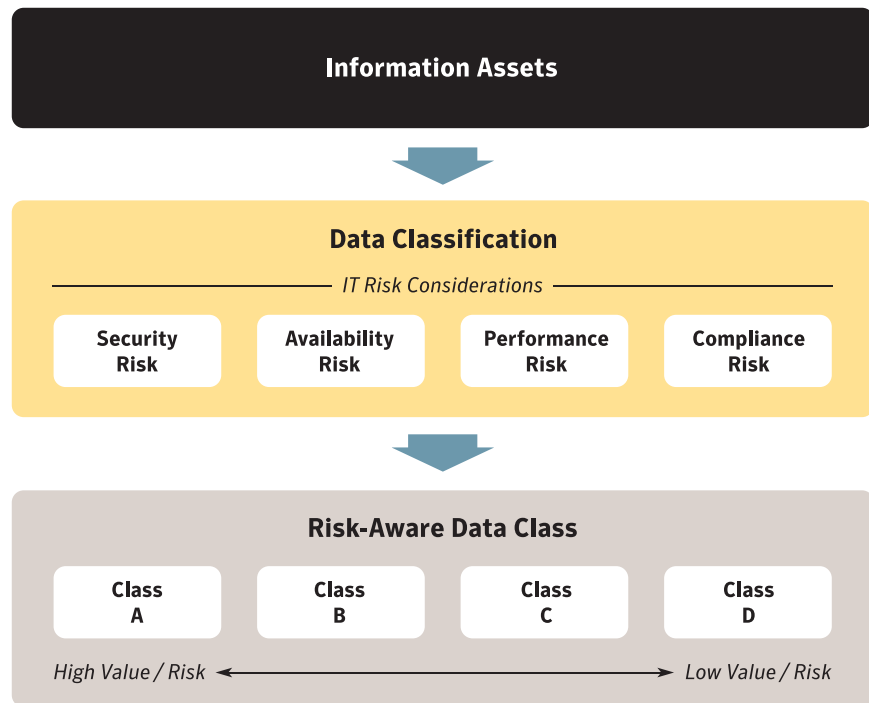


Figure 2: Risk-aware classification groups information assets according to the value they offer or the risks they pose to the organization.

Another core element of Information Lifecycle Management involves the use of metadata to manage information properly over its lifetime. Metadata – information about information² – directs retention and disposal policies to assure that records management follows applicable policies and regulations; it is a key tool for risk managers to mitigate IT Risk using automated and sustainable policies.

A recent example from France illustrates these points. In 2005, the government implemented regulations requiring organizations to retain for 10 years any electronic contracts relating to goods or services valued over €120.³ IT Risk Management programs offer the capability to measure this compliance risk and define appropriate metadata requirements. Without proper metadata for each contract upon creation, association with other documents, and requirements for disposition, it would be difficult or impossible to manage record-retention practices to the required standards.

This example illustrates the importance of using IT Risk Management as a surveying engine for ILM programs, scanning the organization’s legal and compliance environments to identify the full range of risks faced by the organization. Without IT Risk Management to help identify emerging risks and deploy appropriate controls, organizations may incur significant expenses. For example, the SEC has imposed millions of dollars in fines for incomplete email archives in violation of record retention policies under the Securities Exchange Act of 1934.⁴ When IT Risk Management disciplines illuminate and guide ILM practices, ILM metadata and other controls become powerful tools to manage IT Risk.

2. National Information Standards Organization. "Understanding Metadata." <http://www.niso.org>. 2004, page 1.

3. Kahn Consulting, Inc. "Addressing Compliance in Global IT Organizations, Strategies for CIOs and IT Leaders." <http://kahnconsulting.com>. July, 2005.

4. Securities and Exchange Commission. "SEC, NYSE, NASD Fine Five Firms Total of \$8.25 Million for Failure to Preserve E-Mail Communications." <http://www.sec.gov/news/press/2002-173.htm>. December, 2002.

How ILM helps mitigate individual elements of IT Risk

IT organizations need to acknowledge and manage the individual elements or classes of IT Risk – ILM plays a key role in helping IT managers identify, manage, and mitigate each of these risks.

Security risk – ILM data classification helps manage IT security risk, for example, risk associated with an online retailer’s historical credit card information. While the levels of availability or performance risk associated with such information may be low, a security breach that compromises the privacy of this information will hurt a retailer’s brand and reputation, and raise follow-on compliance risk from litigation and regulatory intervention. By considering security risk when classifying information, organizations take preemptive steps to mitigate risk by applying controls like Network, Protocol and Host Security; Authentication; and Authorization and Access Management.

Performance risk – ILM requires matching the type of information storage used to the value of the information stored, a practice called Storage Optimization. This is an important tool for risk managers to manage performance risk with careful application of IT Risk Management controls like Performance Management.

Placing information that is needed often or changed frequently on slow systems to reduce storage costs degrades performance, affecting the speed of critical business processes and cutting productivity. On the other hand, placing all information on fast, high-performance storage systems wastes storage dollars on large volumes of information that do not require this level of performance. Without Storage Optimization, organizations either raise their exposure to performance risk or lose value. Storage Optimization reveals the conflict between risk mitigation and cost, *i.e.*, that reduction of performance risk carries costs that may outweigh its value. Risk managers define how much performance risk an organization can tolerate within budget constraints, then deploy tiered storage to mitigate that risk. Organizations may apply their cost savings from Storage Optimization to fund innovation or enhance IT Risk Management in other areas, or take them to the bottom line.

Availability risk – the concepts of data protection and availability are central to an effective ILM strategy. There are hundreds of ways to protect data, from simple, inexpensive tape backups for basic protection at low cost, to complex replication, continuous data protection, and off-site mirroring techniques that can mitigate almost any availability concern at a price.

System downtime costs the average European organization as much as £300,000 per hour.⁵ Business impacts on this scale raise the urgency of decisions to keep systems available and properly protected. Risk managers define availability requirements for information assets by class, and then deploy data protection technologies and processes based on their business value to manage and control availability risk.

5. Global Switch. "Downtime Costs European Business £300K per Hour." <http://www.globalswitch.com>. May, 2007.

Compliance risk – today's legal and regulatory environments require organizations to maintain and preserve information, often for many years. IT Risk Management and ILM share the goal of ensuring that corporate records are properly captured, preserved, discovered, and discarded from information archives.

The thought of twenty-five year or even permanent archives is unsettling but real: regulatory agencies aggressively enforce fines and penalties for noncompliance with increasingly stringent requirements. In 2006, a leading firm accepted a \$15 million fine for failure to provide email records in an SEC investigation.⁶

IT Risk Management plays a significant role in identifying what information organizations should archive, sorting out related compliance issues, and establishing the role of metadata. Once they understand the requirements, IT Risk Management helps organizations ensure the proper design and maintenance of archives to meet the regulatory needs of the business. Applying ILM controls in a disciplined program of IT Risk Management is fundamental managing compliance risk.

How well are organizations performing?

For its February, 2007 IT Risk Management Report, Symantec asked 310 IT professionals to rate their organizations' effectiveness in implementing a variety of process and technology controls, including ILM.⁷

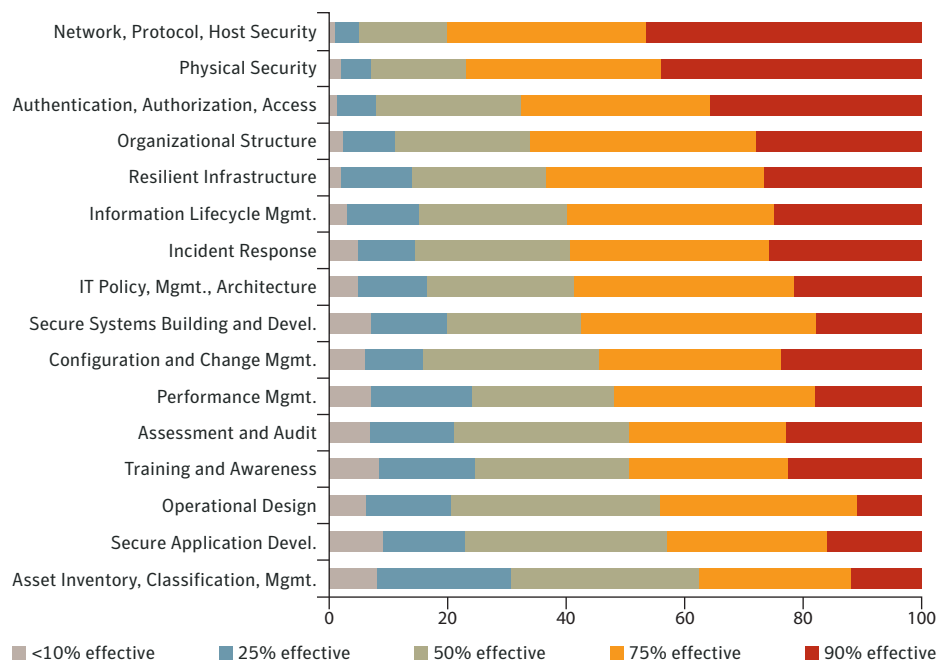


Figure 3: IT Risk Management Report participants' estimates of process and technology control deployments at their organizations, in descending order of perceived effectiveness.

6. Bart Perkins. "Records Retention: Who Cares?" Computerworld. Framingham, MA: IDG Network., April 17, 2007.

7. IT Risk Management Report. Volume 1: Trends through December 2006." Cupertino, CA: Symantec Corporation. February, 2007. The report refers to ILM as "Data Lifecycle Management."

Although ILM ranked in the upper half of all controls for effectiveness, closely-related and supporting controls fared less well. Asset Inventory, Classification, and Management – essential for effective ILM – received the poorest ratings in the study. The discrepancy implies that organizations' ILM processes may be fragmented, or unsupported by the disciplines, skills, and processes needed to make them effective. Alternately, study participants may not have associated the classified information with the assets on which that information is processed, or may have interpreted deployment of commercial ILM solutions at their organizations as proof of effectiveness, even in the absence of essential supporting processes.

In a strong ILM environment, two other controls – Performance Management, and Assessment and Audit – should improve due to the strong emphasis in ILM on service-level management and policy-based archiving. Yet these controls also scored below the midline. The disparity indicates that these organizations have not secured full value of their ILM initiatives, possibly because their managers do not realize the full potential of ILM.

A key finding from the IT Risk Management Report is that the most effective organizations deploy a broad range of technology and process controls rather than concentrating resources on a few high-priority controls. Results for ILM and associated controls indicate many organizations have a long way to go toward this ideal.

Conclusion

Among the many controls available to IT Risk managers, ILM offers great breadth and flexibility, supporting fundamental changes in the management of risk. IT Risk Management should apply ILM to define data protection requirements based on the value of information, and set clear information management policies. By applying ILM as a key control within IT Risk Management, organizations prepare themselves to make proper decisions regarding classification of information and its placement in information stores. Both ILM and IT Risk Management processes benefit from an integrated approach, creating a stronger and more effective IT organization, and improving the risk posture of the organization as a whole.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com

Confidence in a connected world.



For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright© 2007 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of the Symantec Corporation or its affiliates in the U.S. and other countries.
6/07 12489367