

How Do I Manage Information Risk in the Extended Enterprise?

INFORMATION MANAGEMENT OBJECTIVES

These three elements must be kept in balance. Managing information risk is about maintaining this balance.



CONFIDENTIALITY & PRIVACY
Disclosed to and accessible by appropriate entities and processes



INTEGRITY
Maintenance of accurate and complete information



AVAILABILITY
Usable and accessible on a timely basis in the required manner

RISK-BASED MANAGEMENT

Information should be classified; and the likelihood and impact of any breach or failure should be identified, understood, and managed.

High risk information should be managed more carefully; especially as it is transferred outside of the enterprise to business partners and other processors. Lower risk information may be managed with less rigor.

RISKS / ILLUSTRATIVE ACTIONS



HIGH
Visibility, preferably real-time into the control of information.

Documented, third-party assurance about continuous monitoring techniques.



MEDIUM
Contractual obligations about information handling and security.

Periodic certification about system effectiveness.



LOW
Reliance on sound business practices of the partner to effectively manage information risks.

THE INFORMATION MANAGEMENT LIFECYCLE

This model illustrates some events that can throw your objectives out of balance.

1 CREATE / CAPTURE collect, receive

LACK OF CONSENT

While not required in every jurisdiction, obtaining consent from providers and subjects to collect their information is considered to be a best practice.



COLLECT TOO MUCH

Sometimes, in an effort to better manage the business, organizations can generate and collect too much information from business processes, customers, employees and other business partners.

"IT WASN'T US"

Even though third parties may collect information on behalf of the organization, if missteps are made, the organization will be blamed.

2 MAINTAIN store, secure, backup, archive

BROKEN RELATIONSHIPS

It is important to not only store the information, but also relationships with other information. For example, storing both the email AND the attachments. Storing a policy AND links to other policies that it references.

OFFSITE and OUT OF MIND

To effectively address business continuity risks, organizations often store information off-site. You must understand how the partner will handle and safeguard information from attacks and other threats.

SEARCH THIS

Sometimes information can be inappropriately exposed to powerful search technologies. For example, while it may be impossible for a user to browse and find a file, an internal search engine may discover the file, index and cache its contents for all to read.

STORE IT FOREVER

While cheap storage has drastically reduced the cost of technology necessary to store information, the total cost and risk of maintaining too much information must be understood.

Possessing stale, unnecessary data can become a potential liability."

3 MANAGE / USE process, circulate, transmit

e-DISCOVERY

Courts assume that electronic information can (and will) be made available to enforcement and opposing counsel.

WHO OWNS WHAT?

When organizations or business units merge (or dissolve), information ownership and control must be addressed.

- Who owns the information?
- Who has access to it?
- When? How?

TRANSMISSION

When information is transmitted, the security and encryption schemes must be considered.

OUTSOURCED and OUT OF MIND

When business units outsource processes, they sometimes fail to understand how the business partner will handle and safeguard information. Make sure that all outsource partners handle information in a manner consistent with the level of risk.

4 DISPOSE transfer or ownership, destruction

SHRED IN MY BACKYARD

Even the outsourcing of information destruction should be subject to careful oversight. Some sensitive information is legally mandated to be destroyed on premises.

SHRED IT ALL

Computer systems and components such as disk drives may require physical shredding to ensure information is not inappropriately disclosed.



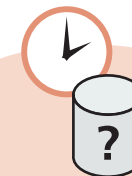
TRANSFER of OWNERSHIP

Ownership of information may be transferred to other organizations or even the government. Make sure that copies as well as originals are either destroyed or transferred.



SUNSET CONTRACTS

Some information lives under contracts specifying that it will be destroyed after a period of time. Make sure that all copies are managed and disposed of as well.



AFTER ITS TIME

Retaining information long beyond its usefulness increases the risk that information may be inappropriately used.

BEFORE ITS TIME

Accidentally disposing of information before it is time may lead to both business and legal risk.

UNAUTHORIZED DESTRUCTION

Disposing of information inconsistent with documented retention schedules or, worse yet, in contravention of a "legal hold" or other specific request.

CHEAT SHEET

These are just a few of the laws, standards and guidelines that can be used to model an information management program.

STANDARDS / GUIDANCE

- ISO 15489. International standard for records management.
- AICPA GAPP. Information privacy standard set by the American Institute of Certified Public Accountants.
- DoD 5015.2. Standard set by the U.S. Department of Defense requiring any contractors to handle sensitive information using specific practices. While focused on DoD contractors, this standard presents best practices than any organization can use.
- US Federal Rules of Civil Procedure eDiscovery Guidelines detail expectations for producing electronic records and documents for legal matters.

LAWS

- EU Data Protection
- Canada's PIPEDA
- US GLBA, HIPAA and Safe Harbor Provisions
- US FTC Fair Information Practices Principles
- USA PATRIOT Act
- US Federal Information Security Management Act
- SOX Act of 2002

DEVELOPED BY



DEVELOPMENT PARTNER



©2008 OCEG®

XPLANATIONS™ by XPLANE®

contact info@oceg.org for comments, reprints or licensing requests