

# *synnovation*



Vol. 1 Issue 3

## Beating the Odds

Leading an organization through a risk-laden environment is often a game of chance. But enterprise risk management can help your odds.

### EDS

Unwelcome Surprises

By Al Decker

### Towers Perrin

Coming of Age

By Prakash Shimpi

### Microsoft

Defending the Crown Jewels

By Ron Markezich

### Oracle

Protect, Detect, Deploy

By Vipin Samar

### Dell

Super Power

By Dr. Reza Rooholamini

### Sun Microsystems

Tapping Tag Power

By Jim Del Rossi

### Xerox

For the Record

By Charles P. Brett

### EMC

Reaching Out

By Gregg Therkalsen

### Cisco Systems

A Matter of Self Defense

By Bob Gleichauf

---

### EDS

Conversations

With Ron Rittenmeyer

### Microsoft

Up Close and Personal

With Ron Markezich

# For the Record

## Enterprise Records Management is Crucial to Keeping Enterprises in Check

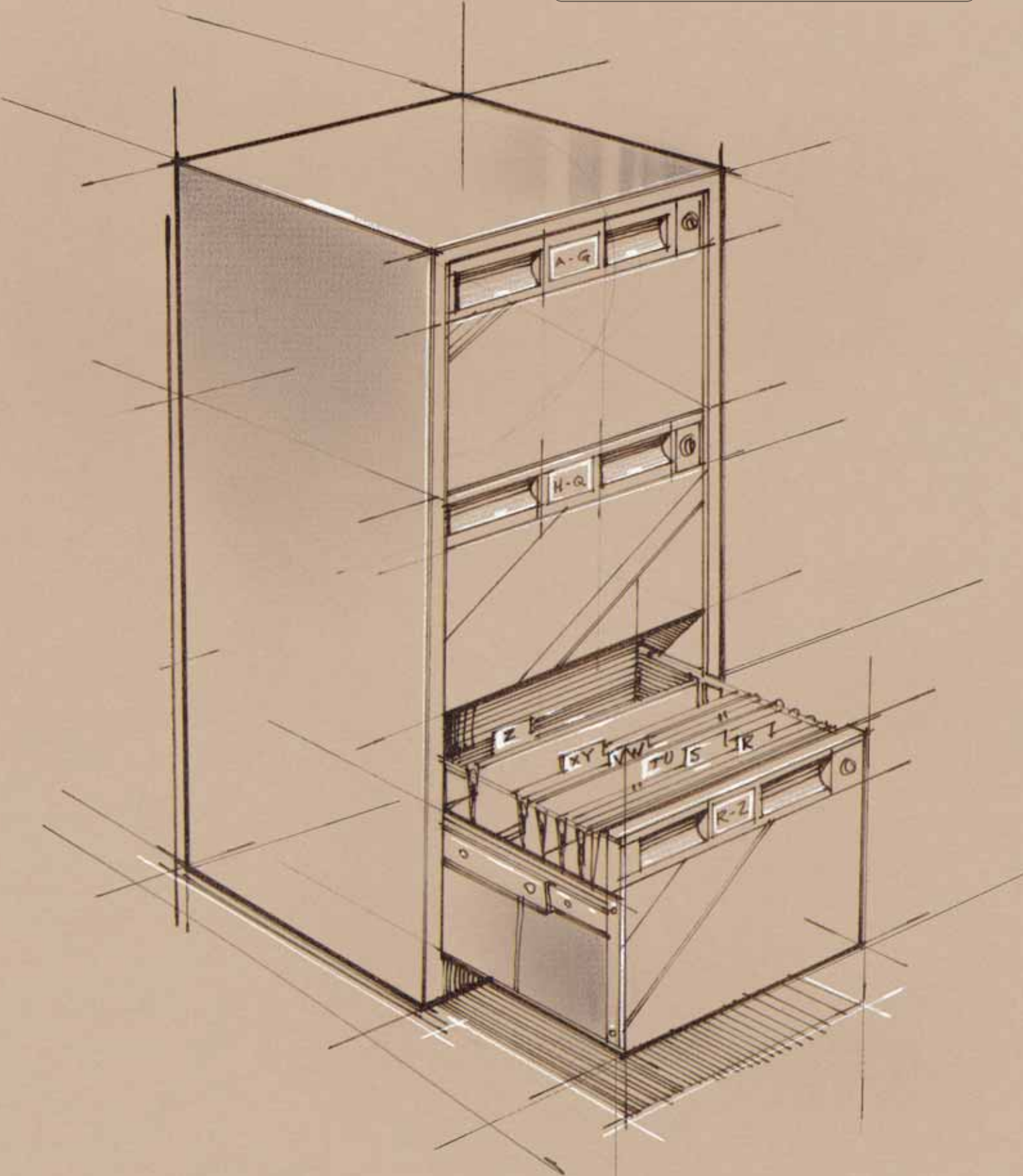
BY CHARLES P. BRETT, XEROX CORPORATION

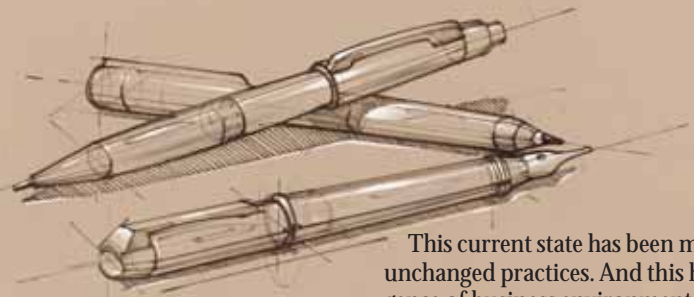
**E**nterprise records management has always been a party to risk mitigation, but its stature is now gaining prominence across enterprises everywhere. For most, keeping the right records safe (or not doing so) is a bit sexier than our old image of a room full of filing cabinets. Legal precedents established in the past few years have placed heavy burdens on both sides of lawsuits to produce documents for audits, litigation, or discovery matters. Even so, only a relatively small percentage of businesses and organizations are administering enterprise records management correctly, or, at the minimum, are on the right track.

In practice, solid records management enables faster, flexible, complete, and more secure organization-wide location, retrieval, and use of information regardless of geography, medium, or system type. And these principles must support business needs, privacy issues, and other access security considerations. Further, these systems and processes support and ensure preservation of an authoritative record of the enterprise's decisions and actions, as long as it's required to support research and program needs, protect customer or public rights, and safeguard enterprise accountability—which in some instances requires permanent preservation of

hardcopy and electronic records.

Leveraging technology to improve services, reduce costs, improve security, and reduce physical-based information silos (paper, microfilm/fiche, etc.) has become a way of life within many enterprises. But with this shift, new concerns have risen. These concerns include the lack of tools for centralized discovery, a shift toward use of electronic systems (such as e-mail) as the primary medium of communications by organizations, and a general lack of consideration within the systems for comprehensive management of the mass of records created. >>





This current state has been maintained by unchanged practices. And this has led to the emergence of business environments characterized by the following:

- Increased copying, modification, and storage of electronic records and hardcopy versions across organizations, applications, and media, with an accompanying escalation of costs associated with storage and use.
- A difficulty in locating and identifying authoritative versions of documents. This is often associated with absence of data that enables users to determine a given record's origins, level of approval, or whether it's the latest, most complete, or relevant version.
- A lack of a common repository to show what records and data exist and where. They are often inaccessible on users' hard drives or buried in individual or corporate file systems—all with absence of authoritative directories of information at the enterprise, line of business, or even working group level.
- Requiring separate and distinct search processes for structured data, desktop records, and hardcopy records, associated with an overall tendency to manage information resources according to their physical form rather than as information.
- Utilizing manual processes to prevent the uncontrolled deletion of electronic records by users and unauthorized disposal of hardcopy records.

#### Records Management

The areas of focus for a records management program will impact areas where the enterprise perceives the greatest amount of risk toward records management and business continuity. The risk profile for determining records requirements will provide guidance to enterprise records management for current and future needs. In general, a risk profile is a systematic and thorough identification of records-related risk, enabling a measured approach to business continuity: a sound approach to scoping the boundaries of the problem, determining the issues within those boundaries, and making decisions about solving the problem. In general, three areas have been identified: compliance, reputation, and strategic. A risk profile approach to records management—inclusive of retention and compliance, litigation pre-

paredness, disaster recovery, and business continuity—employs a broad, systematic, and rigorous approach:

- Identify issues and establish a management framework
- Identify and characterize exposure and vulnerabilities, and develop evaluation criteria
- Profile and evaluate risks
- Identify, evaluate, and recommend risk mitigation strategies

#### Compliance Risk

Compliance risk is the current and prospective risk arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies, procedures, or ethical mandates. This risk exposes the enterprise to fines, penalties, payment of damages, voiding of agreements, and adverse inference, among others. Compliance risk can lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and an inability to enforce contracts and agreements. To mitigate compliance risk, records and risk managers should make an assessment of the organization's compliance environment to determine:

- Does the enterprise have a satisfactory record of compliance? Are records management systems adequate enough to avoid significant or frequent violations or noncompliance?
- Do violations or noncompliance expose the company to significant impairment of reputation, value, earnings, or business opportunity?
- Does management fully understand all aspects of records compliance risk and demonstrate a clear commitment to compliance?
- Are authority and accountability for risk management clearly defined and enforced?
- Are records management considerations incorporated into system development and modification processes, including changes made by outside service providers or vendors?
- Are training programs effective, and have the necessary resources been provided to ensure compliance?
- Does the enterprise records management policy fully consider legal and litigation requirements?

# A holistic approach to enterprise records management is recommended.

## Reputation Risk

Reputation risk is the current and potential impact on earnings and capital arising from negative public opinion, affecting the enterprise's ability to establish new relationships or services, or continue servicing existing relationships. This risk may expose the enterprise to litigation, financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise caution in dealing with its customers, shareholders, the community, and other stakeholders. To mitigate reputation risk, managers should make an assessment of the organization's risk environment and determine:

- Does management anticipate and respond well to changes of a compliance or regulatory nature that may impact its reputation in the marketplace?
- Does management foster a culture of compliance that's well-supported throughout the organization and has proven very effective over time?
- Are strategic initiatives supported by sound due diligence and strong risk management systems and procedures? Can decisions be reversed with little difficulty and manageable costs?
- Does the enterprise regularly experience litigation or frequent customer complaints?
- Are internal records management control and audit generally effective?
- Has the enterprise avoided conflicts of interest and other legal or control breaches? Is the level of litigation, losses, and customer complaints manageable and commensurate with the volume of business conducted?

## Strategic Risk

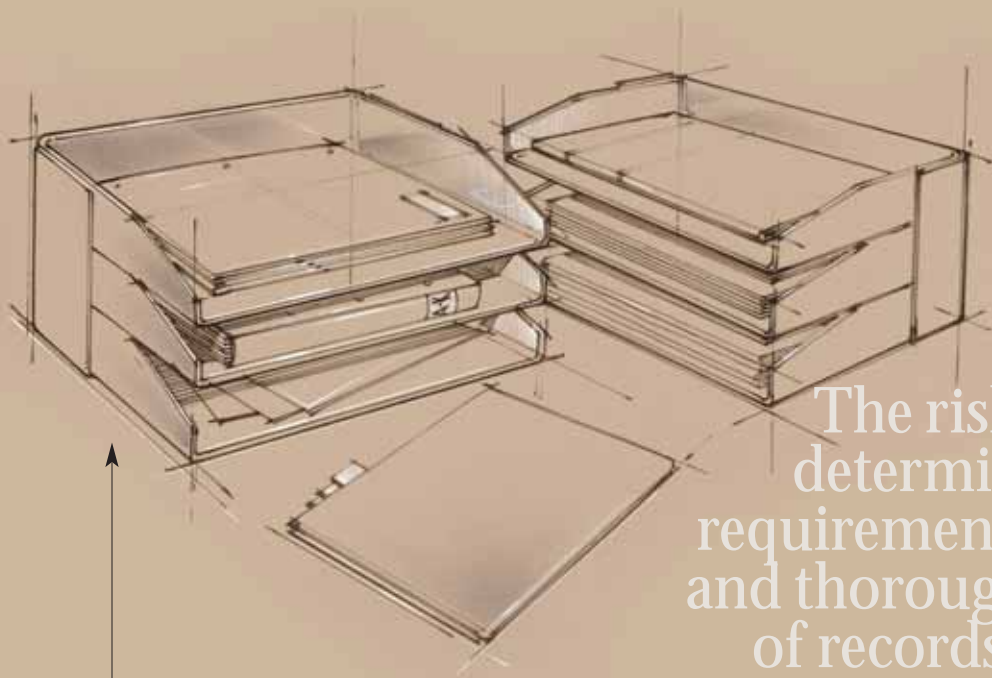
Strategic risk is the current and prospective impact on growth and expansion arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry or market changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against the goals, and the quality of implementation. The resources needed to carry out business strategies include communication channels, operating systems, delivery networks, and managerial capacities

and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, and other environmental changes. To mitigate strategic risk, risk managers should make an assessment of the organization's risk environment and determine:

- Is records management within risk management practices an integral part of strategic planning?
- Are strategic goals, objectives, corporate culture, and behavior effectively communicated and consistently applied throughout the enterprise?
- Has records management been successful in accomplishing past goals and is the practice appropriately disciplined?
- Do records management policies and systems effectively support strategic direction and initiatives?
- Do records management and litigation exposure reflect strategic goals compatible with business strategies?
- Do deficiencies in management decision-making and risk mitigation preclude the enterprise from effectively evaluating new products, services, or acquisitions? >>

## Enterprise Records Management: Doing It Right

1. Establish ownership and accountability
2. Know when and how to retain records you must keep for legal, regulatory, and statutory reasons
3. Know when to dispose of records
4. Develop a system for keeping records that balances the time and cost associated with keeping them and the value of the archival information
5. Create an efficient way to store and retrieve records
6. Keep records safe from unauthorized access, alteration, removal, or destruction
7. Know what records you don't need to keep at all, which saves time and money because you'll avoid unnecessary collection and maintenance



The risk profile for determining records requirements is a systematic and thorough identification of records-related risk.

#### The Costs of Avoidance

For many organizations, existing processes have not yet addressed the risks associated with improper records management, nor will redesigned manual processes enable efficient and effective management of records. Currently, few enterprises enable consistent and enforced processes, procedures, or the information technology tools that allow them to ensure that information resources are accessible by staff, subsidiaries, and business partners. In particular, it's making the right information available at the right place at the right time, not only within individual programs and global processes, but also across those processes as well.

Enterprises also need to apply systematic rights of access to ensure the most appropriate use of individual resources—protecting the evidentiary integrity of official records and reducing the costs associated with accessing, managing, and storing resources. It's also important to assign appropriate management accountabilities to information resources to help ensure that records with ongoing value are protected against premature disposal, and records with permanent value are transferred to the enterprise archives (i.e., off-site).

The reality is that most enterprises don't have comprehensive plans for the systematic management of physical and electronic records, and this exposes them to a number of risks, including:

- Loss of records by failing to capture them when they're created (due to technology obsolescence or a lack of intellectual control)
- Inability to manage alteration issues due to decentralized electronic recordkeeping
- Inability to proactively or defensively locate "smoking gun" content, possibly within e-mail systems
- Business managers and IT system administrators don't specify recordkeeping requirements when systems are designed/upgraded.
- System administrators assuming the role of electronic record archivists partly because there's no practical, consistent advice on how to proceed, and partly because some business system administrators view the records in their systems as "their" documents or data. This results in a number of decentralized shared drives/repositories of electronic records with various degrees of quality control and access.
- High costs and difficulty in meeting regulatory, discovery, and litigation deadlines
- Enterprises continue labor-intensive, case-by-case mapping of paper record retention schedules to electronic records.
- Enterprises focus only on those electronic records within immediate view and lose sight of an enterprise-wide strategy for those records with potentially greater business, legal, and research value.

### Critical Success Factors

A holistic approach to enterprise records management is recommended, taking into consideration business culture, process, and technology to create a valuable program. Overall, it's important to remember that records support business and the way people conduct business, not the converse.

Sound processes built on easy-to-understand, accessible policies and procedures are key for ensuring compliance and mitigating risks. Moreover, while technology is important, it only accounts for a small portion of what's required to implement and maintain a records management program.

The scope of most risk management projects is to create a records management policy for the enterprise that will comply with all regulatory requirements, meet the organization's business needs, and provide overall accountability. The program must include all media defined as a record, which may include paper, electronic records, and all other relevant media such as microfilm.

There are a number of goals for any integrated system of processes and technology that support business records. By automatically ensuring that these goals have been embodied in the solution, enterprises can dramatically improve the consistency and effectiveness of their records management programs. These critical requirements include:

- Timely disposal or archival of recorded information per the enterprise retention guidelines
- Ensuring efficient storage and retrieval of recorded information under control or custody
- Ensuring that recorded information is protected from unauthorized access, alteration, removal, or destruction
- Eliminating unnecessary collection and maintenance of stored or recorded information
- Ensuring the timely transfer or disposal of recorded information in accordance with enforced retention schedules and enterprise-wide standards

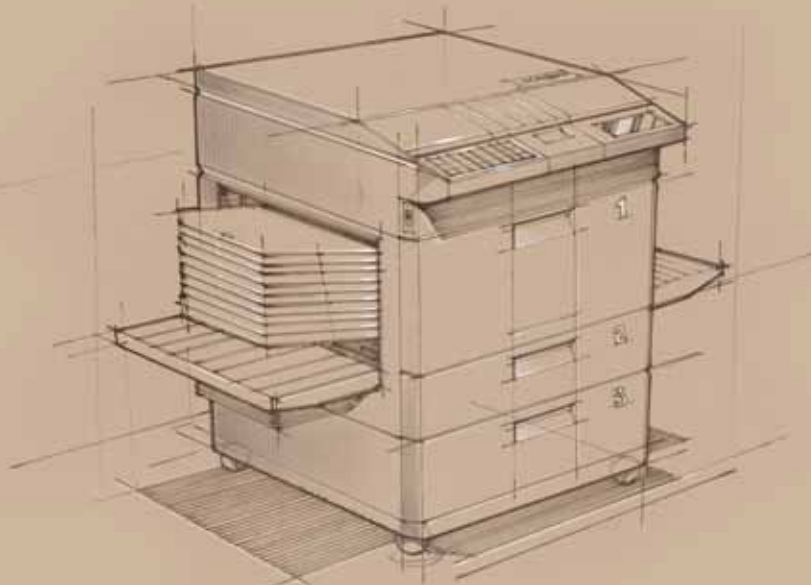
### Implementing an ERM Plan

Following are some specific steps that will help you implement an effective enterprise records management program. >>

## Enterprise Records Management: Misdirection and Pitfalls

Many organizations aren't doing what they need to in the area of enterprise records management. Here are 10 common mistakes:

1. Organizations avoid the entire issue, making themselves vulnerable to an event that could make enterprise records management—or the lack thereof—suddenly vitally important. Don't wait for such an event to sting you. Be proactive.
2. Enterprises aren't engaging the right people within the organization, including legal, HR, and IT. You need to get the right people involved, including the right stakeholders.
3. Many organizations don't have enforcement from the top to get the message out. Executives must make it known that this is an important project.
4. Many companies aren't putting enough resources into the project. It isn't enough to assign a system administrator or paralegal to handle this on his own.
5. Enterprises aren't seeing the systems already in place to begin the process.
6. Organizations are focusing too much on one business process or area instead of nurturing a more global perspective. The idea is to ensure that the right information can be accessed at the right place at the right time—not only within individual programs and global processes, but also across those processes.
7. Organizations aren't coordinating IT with the rest of their business, which leads to a disconnect between each department's records and processes.
8. Enterprises aren't sharing storage systems and procedures with all parts of their organizations.
9. Enterprises aren't looking at records management in the overall risk compliance framework, including risk management, litigation, and legal.
10. Enterprises aren't creating a synergy between other related technologies, such as disaster recovery, e-mail, and backup.



**Define and Measure**— to determine which records are being kept, both in paper and electronic form. This assessment should employ methodologies that use special information-gathering techniques to capture the very essence of an organization's work processes. The result will provide a clear road map for navigating the next enterprise records management elements.

**Prepare for Change**— Identify and train for risks that are to be remedied by implementation of the program, as well as applicable laws or regulations requiring user action. This must come from the top level of management. Documents, records, corporate knowledge, and storage policies must be balanced throughout the workplace. This involves employees, the way an organization conducts its business and supporting process, and how technology enables the flow of business and supports records management functions.

**Pick a Program**— As the vast majority of enterprise records content is in both physical and electronic formats, the selection of a single vendor offering integrated solutions is highly recommended —active involvement of the IT organization is mandatory at this step. The complexity of tools and procurement process is maturing, though they aren't necessarily straightforward. Organizations must develop a comprehensive approach to records—including physical, electronic, and data center operations. They must also determine the appropriate balance between data requirements and the flow of the business, minimizing disruptions to employees' daily routines.

**Give Your Program a Test Run**— A pilot implementation should focus on business areas that are considered the most exposed, that are immediately reactive to events (litigation, audit, etc.), or that may minimize risks associated with current enter-

prise records management practices. Develop a common taxonomy model, because most corporate content is created, accessed, managed, and reused across many parts of the organization.

**Embrace a Full-Scale Program**— Enterprise-wide implementation and collaboration with multiple lines of business within the organization will become necessary. The organization should also address other existing enterprise content applications, such as imaging, document management, ERP, etc. In the future, any new content-related initiatives must include input from the enterprise records management team.

**Assess, Measure, and Refine**— Prepare your organization for the changes you've implemented. An inclusive approach to enterprise records management is critical if you hope for long-term success. Such an approach requires consideration of all aspects of organizational culture, business processes, and technology to create a sustainable program that provides maximum value to your organization. Sound processes, built on straightforward, accessible policies and procedures, are key for ensuring compliance and mitigating risks related to litigation, discovery, and regulatory compliance.

#### **With Risk Comes Rewards**

You may think of all this as a cost of doing business, and certainly that's one way to look at it. But implementing sound records management policies, procedures, and technologies on both a strategic and infrastructure level can demonstrate a return on investment. Such programs can reduce response costs and access, create a single point of entry for all corporate records, minimize data and records stored in multiple systems, and improve overall business if addressed strategically.

By adopting best practices, and creating a culture of risk awareness, enterprise records management will help your enterprise:

- Support better decision-making and strategic planning through improved public access to your information services, improved client service delivery, and leveraging of efficiencies through multi-channel service delivery
- Reduce the costs associated with management and use of your enterprise's paper-based information resources and improve the capture, preservation, and sharing of critical information
- Enhance your organization's accountability and transparency through improved access to and preservation of such records
- Increase reliability through authoritative versions, while preserving and assessing the authenticity and relevance of records, and protection against unauthorized or undocumented alteration
- Avoid risk through ensured preservation of records required to document rights, liabilities, and responsibilities, and demonstrate the content and rationale for decisions, as well as improve access to information required to prevent policy design and delivery errors
- Enhance information security through comprehensive, secure, and precise assignment of access permissions
- Improve consistency and responsiveness to audit, litigation, and discovery demands

Many enterprises are playing catch-up to ensure that risk mitigation—including records management—joins the ranks of other business functions or units, such as IT, operations, ethics, compliance, audit, and finance. We're learning that we already have risk management practices within our organizations, but they're highly specialized and not necessarily coordinated. And they focus on specific systems or functions.

Five to 10 years from now, there should be a vast awareness that organizations must look at risk in a more holistic way. That's when we'll integrate some of these pieces, finally entering the value-risk optimization phase and giving this not-so-new concept its due respect. |s|

About the Author: **Charles P. Brett** is a managing principal for Xerox Global Services.

## Records to Risk Continuum

### 1990s

- Paper and electronic records converge
- Imaging, document management, and workflow emerge
- TIFF and PDF recognized as long-term file formats
- Records management expertise expands
- Distributed systems, PCs, and e-mail become standard
- Electronic content admissible by law
- "Structured vs. Unstructured Content" concept airs

### 2000-2007

- September 11 and natural disasters
- Risk management on the radar screen
- Financial scandals and corporate misconduct
- SOX, PATRIOT, HIPAA, GLBA, etc.
- E-mail confusion and misuse
- Cross-functional records management begins
- Records management moves mainstream

### 2007 and beyond

- Enterprise risk management
- Stakeholder recognition
- New C-level concerns: compliance, risk, information security
- Records management formalized and accountable
- Enterprise content and records as infrastructure
- Risk and records management methodologies harden
- Enforcement and refining

