Date: Jan. 12, 2010

Item No. 3
File No. _____

SUNSHINE ORDINANCE TASK FORCE

Compliance and Amendments Committee

AGENDA PACKET CONTENTS LIST*

☒	**Developing e-document retention policy**
☐	
☐	
☐	
☐	
☐	
☐	
☐	
☐	
☐	

Completed by: Chris Rustom **Date:** Jan. 7, 2010

***This list reflects the explanatory documents provided**

~ Late Agenda Items (documents received too late for distribution to the Task Force Members)

** The document this form replaces exceeds 25 pages and will therefore not be copied for the packet. The original document is in the file kept by the Administrator, and may be viewed in its entirety by the Task Force, or any member of the public upon request at City Hall, Room 244.

Evaluating "Best Practices" for Electronic Document Management: Tips for Ensuring Successful Implementations the *First* Time

View printable PDF (opens in new window)

It's a pretty safe bet to say that most people who are worth their salt want to do things right the first time. In a field such as electronic document management (EDM), which has advanced significantly in the past two decades, discovering true best practices that lead you onward toward success can feel like chasing a moving target with your eyes closed. Although there is no shortage of opinions, it has been historically challenging to find agreement on what constitutes best practices. Ensuring that your vendor meets expectations is difficult if standards are unclear or not clearly communicated.

This article gives an overview of best practices, and practical considerations as you consider purchasing and implementing an EDM solution. It provides a synopsis of typical components in an EDM suite and useful tips for choosing solid solutions that deliver what they promise. It also outlines challenges and recommendations for evaluating vendor "best practices" and cites several reliable sources for information about industry-wide best practices in EDM. The goal of this article is to help EDM project champions and managers evaluate technology providers with open eyes and make the right decisions the *first* time so they can experience maximum payoff and satisfaction from their investment.

Defining best practices

Best practices in EDM involve stating the guidelines, or methodologies, that are needed in order to ensure that the best solution is chosen for a specific business challenge and that the implementation is delivered in the wisest manner possible. Typically, true best practices are defined by a respected, independent authority or industry association as a result of commonly stated challenges, experiences, and lessons learned from successes and failures. They help to encourage frequent repeats of success and avoidance of disappointment and failure.

In order to engage in and deploy best practices, a company has to take a holistic approach to the business challenges and the goals of the stated project. Otherwise, the solution will never rise beyond the implementation of multiple narrow, departmental solutions. Best practices for EDM involve choosing the *best* technology that is available to solve a specific business challenge and meet clearly defined project goals. Ideally, these guidelines help companies to set clear and realistic expectations for EDM, as well as detailing project deliverables and spelling out how any project-related issues will be resolved. Best practices help companies to make decisions that lead to successful implementations the *first* time.

Typical components in a standard EDM solution and practical tips to consider

1. Capture

The foundation of any EDM solution is the effective capture of all of your corporate information, regardless of its source. Information enters a company in multiple ways, from paper documents to online forms, bar codes, copiers with basic scanning capabilities, emails, faxes, electronic signatures, and more. Capturing all of the data and storing it in a central repository is the foundation to organizational efficiency. Before you select a vendor, make sure you understand all of the sources of information collected by your organization and the volume that is received from each source. Examine the type of technology that you need, and make sure it can accommodate all types of input.

Can your vendor key in necessary data from an image? Is the company able to ensure that the images are secure, so that keying can be done remotely or overseas and still preserve its integrity? Is your vendor able to capture all formats and present high-quality definition and readability, including documents created in Microsoft Word, Corel Perfect Office, email, drawing packages, Web pages, and others? Do you have an off-site backup facility or alternative to ensure that your mission-critical data will be available in the event of negative unforeseen circumstances?

2. Taxonomy

After information has been captured, it needs to be indexed and stored for easy and secure retrieval when it is needed. A company with multiple departments or types of users may need to consider a thorough and hierarchical taxonomy in order to index information in diverse ways so that multiple people can find what they need. Mr. John Doe's personnel file may have data that is pertinent to the HR department, other information that is needed by the payroll department, and facts that are needed by the marketing department. His company needs to see that the right people can access what they need...no more, and no less. Does your vendor's EDM package allow you to index information as thoroughly as you need in order to make the information easy to find for everyone who needs it? Does it also guarantee security?

3. Document Management and Security

As data is entered into the system, rules governing privacy and sensitive information need to be followed. The client needs to determine and communicate to the IT administrator who is allowed to view which information, taking government regulations, industry standards, and corporate policies into consideration. Does your vendor provide a solution that lets you designate who can view which information, down to the individual user and at the page level? Does the software allow the client to set up user authentication? Can documents be made to be inalterable? Does the system provide a clear record of access that is auditable?

4. Business Process Management/Workflow

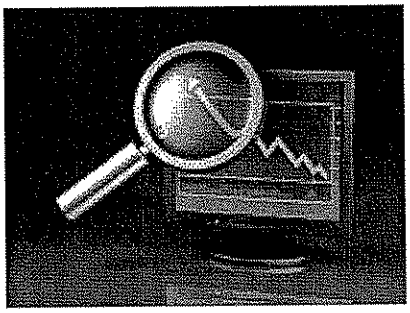
There are many best practices to consider with regard to BPM and workflow. One common requirement that is addressed by such guidelines—but otherwise frequently overlooked—is the need to establish and communicate clearly *who* is responsible for making the business rules that govern automated processes. A client is responsible for communicating a clear hierarchy of responsibility and decision-making for every process,

but who at the site *specifically* has the final say for choosing and communicating the business rules?

Does the software you have selected have the ability to create a clear hierarchy for decisionmaking, including authorization not only at the department level, but at the individual level? Does it allow you to designate how exceptions will be handled? Are each of the transactions within processes that are "on the move" fully searchable and instantly auditable when immediate answers are required?

5. Records Management

A document becomes a record when it has completed its active lifecycle, is no longer likely to be needed on a regular basis, and is ready to be stored for the long-term. Companies need to do more than take into consideration the regulations and policies governing document retention, although this is a vital first step. Creating a clear and consistent file plan for organizing records, similar to a taxonomy for indexing information in the active life of a document, is essential to finding a record when and if it is needed in the future.



Who is authorized to establish and communicate the rules about automatic purging of records from the document management system, or their migration to long-term storage? Does the vendor's software enable the client to request email notification or other alerts prior to purging data? Will the client require alternative long-term storage media for records in addition to electronic storage? If so, does the EDM vendor's software export data effectively to the chosen media? If data needs to be destroyed ultimately, does the vendor have the capability to dispose information and hardware properly, or a strong partner that the company can recommend for this service and with which their products can integrate?

6. General rules for successful technology deployment

Although the best course of action will vary from one type of deployment and technology to the next, there are some practical strategies that are wise for all technology deployments:

- choose a vendor whose software is truly based on open architecture so that they can integrate with applications you have now *and* software you might purchase in the future;
- establish a clear, written communication of expectations from the client to the vendor;
- require equally clear, written communication from the vendor of expectations the *client* must meet prior to technology deployment;
- generate a schedule of regularly planned status reports from the vendor and client, and make sure they are delivered in a timely manner;
- create a list of project milestones with estimated dates for completion of each, and scheduled communication as each milestone is met; and
- document the vendor's suggestions and client's plan for maintaining the technology (upgrades, etc.) after the deployment is complete.

7. Practical tips for broadening the scope of a technology deployment

Similar to a home renovation, a technology deployment can easily become endangered by the discovery of additional wishes and needs that are beyond the scope of the initial project plan. Project managers and vendors need to be careful only to add whatever is crucial to reaching the project's stated goals. Although it is easy to insert freshly discovered dream lists after the project plan is in place, costs can spiral out of control because of the impact that additions beyond the scope of a project can have on hardware, software, upgrades, staffing needs, and more. Only add what is crucial to reaching the current project's goals. Other items can be added, but only as separate projects with their own stated deliverables, timelines, and budgets.

Challenges and solutions for evaluating "best practices" from vendors

Until fairly recently, "best practices for EDM" have primarily been created by vendors, with recommendations that were more closely related to what each vendor anticipated being *able* to deliver rather than what was truly needed and expected by the client. As a result, some companies that are considering EDM solutions (or that already have one and are not fully satisfied) look with suspicion at vendor "best practices". In the early years of EDM, many vendors promised to provide solutions that would finally address commonly faced business challenges, and then failed to deliver on their promises.

Three areas in which many vendors fell far short of expectations were the promised delivery of centralized information management; a global repository of services; and intelligent process infrastructures. Companies too frequently made major investments that ran into millions of dollars, yet the resulting solutions often remained proprietary or had inherent restrictions that limited the ability to provide the true global information and intelligence they were seeking. As a result, many companies ended up with multiple, isolated solutions that served the needs of diverse departments, rather than a solution that integrated all of their corporate information and provided the global intelligence that managers were seeking. "Buyers, beware" became an unspoken mantra.

Sources for information about industry-wide best practices in EDM

In recent years, organizations such as AIIM (Association for Information and Image Management – www.aiim.org), NARA (National Archives and Records Administration - http://www.archives.gov/), and ARMA (Association of Records) have worked hard to create, document, and publish industry standards for document management and its sister component in the document lifecycle, records management. These organizations have published numerous best practices articles, and offer links to valuable sources of information about document and records management, integrated document and records management, and technologies that are built on an EDM foundation such as digital workflow. In addition, they offer certifications such as CDIA+ (certified document imaging architect) as well as fundamental and advanced document and records management classes, business process management seminars, and other coursework.

Although the vendors you evaluate should be able to provide you with valuable information to help your project be successful, the industry associations provide a broad and unbiased perspective that may help you develop objective, clear, and realistic expectations for the technologies you choose and for each project. Understand the industry standards that are being set by these organizations. Add the vendor's guidelines to your knowledge base. Evaluate how closely your chosen vendors' products and

guidelines meet industry standards. Choose wisely and plan carefully by evaluating best practices for EDM the *first* time. If you do all of this, you are bound to reach your goals.

http://www.docfinity.com/reference/EDM_Best_Practices_Article.htm

A SURVEY OF FEDERAL AGENCY RECORDS MANAGEMENT APPLICATIONS 2007

A Records Management Study Prepared by:

National Archives and Records Administration
National Records Management Program

Table of Contents

1.0 EXECUTIVE SUMMARY 1

2.0 PURPOSE 3

3.0 METHODOLOGY 4

4.0 RECORDS MANAGEMENT APPLICATIONS 5

5.0 SURVEY RESULTS 7

5.1 AGENCY A: SURVEY RESULTS 7
5.2 AGENCY B: SURVEY RESULTS 13
5.3 AGENCY C: SURVEY RESULTS 19
5.4 AGENCY D: SURVEY RESULTS 24
5.5 AGENCY E: SURVEY RESULTS 27

6.0 CONCLUSIONS 31

APPENDIX A – QUESTIONNAIRE 34

APPENDIX B – NPS CASE STUDY 38

APPENDIX C – EMAIL ARCHIVING SCENARIOS 40

APPENDIX D – GLOSSARY 43

APPENDIX E – REFERENCES 45

1.0 Executive Summary

In 2007, a National Archives and Records Administration (NARA) team surveyed five Federal agencies who are implementing Records Management Application (RMA) software products to manage their electronic records. The survey team interviewed Records Officers from each of the agencies and had them complete a questionnaire on the progress they are making with their RMA implementations. **NARA** provided feedback about its own RMA as did the following agencies:

Nuclear Regulatory Commission
U.S. Department of Defense, U.S. Navy, Naval Criminal Investigative Service
U.S. Department of Energy, Bonneville Power Administration
U.S. Government Accountability Office

The following report summarizes the survey responses agency-by-agency, covering the relative successes or (mixed-successes) of the software products against agency-defined expectations. Much of the information was derived from the questionnaire which focused on impact of the RMA implementations in terms of the records management programs, IT operations, and agency employees who administer and use the software. The final section draws some conclusions from these responses.

The survey results do not yield any major surprises. Generally, each of the agencies is satisfied with their software product and how it operates in program and administrative offices. With one exception, the RMAs are performing up to expectations in capturing, categorizing, and storing electronic records and employees are making use of their RMAs to file their electronic documents including "record" email messages.

Most of the agencies surveyed have the following characteristics:

- Senior management support for the RMA implementation;
- Employee population of 3,200 or less;
- Committed headquarters records officers, records management staff, and liaisons who have been well educated in the functions and operations of the RMA;
- Users who are more comfortable in operating the RMA for records management because the agency already is using document management, collaboration, portal, or other technology from the same or other vendors;

- Agency culture that emphasizes the value of documenting work processes;
- Predominantly case file-based records series;
- Track record of piloting document or records management software prior to acquiring their current RMA product;
- Sound records management programs and policies already in place;
- Adequate level of user tolerance for performing daily electronic filing.

The survey results lead us to conclude that:

- Properly employing an RMA can take years of effort and resources for planning, testing, and implementing the system;
- Conducting a pilot and using a phased-in approach to implementation works better than rolling out the RMA software to all users at the same time;
- The product must be easy to use and as transparent as possible;
- The right level of promotion and training during the RMA implementation can help successfully win over those who will use the software for recordkeeping;
- Close attention paid to individual users in the learning phase is critical;
- Creative strategies such as the use of flexible scheduling and reducing the number of users who have to file record email messages can help facilitate the RMA implementation;
- The RMA technology must integrate with other applications and the operating system, especially with the email system;
- Implementing an RMA seems to be less about the functionality of the software product itself and more about other factors such as agency culture, the quality of the records management system in place, user buy-in, etc.
- Further study should be made of Federal RMA implementations, and beyond that, of technologies that are being used to manage email.

This survey does not imply that the techniques and strategies used by these few Federal agencies will automatically translate to success for all other offices and departments of the Federal Government. There are no vendor product ratings or comparisons included. Agencies are free to analyze the responses provided by the entities who cooperated in this study to help determine if an RMA is a good fit for their situation, and if not, consider other alternatives.

Sarbanes-Oxley's Document Retention Rules and Best Practices
Presented by: Thomas Mrva, President & CEO, Lighthouse Computer Services, Inc.
Date: October 27, 2005
Time: 1:00 – 2:30PM

Part 1: The New Record Retention Rules Under Sarbanes-Oxley

INTRODUCTION

- When Congress passed the Sarbanes-Oxley Act (SOX) in July 2002, it imposed new accounting and financial reporting requirements on publicly-traded companies.
    - This impacts all companies traded on US exchanges with revenues in excess of $75 million – it also guides private companies to some degree, and we'll cover that as well.
    - Since the passing of SOX, companies have been scrambling to revamp their accounting processes and systems to ensure compliant financial reporting.
- Compared to most Congressional Acts, SOX is fairly brief at just 66 pages, and yet thousands of pages have been written about how this Act affects businesses, both public and private.
    - Some of the most important sections of SOX create strict new rules about how companies must manage their records – and SOX takes a very **broad definition of the word "records".**
    - A record is essentially any material that contains information about your company's plans, results, policies or performance. In other words, anything about your company that can be represented with words or numbers **can be considered a business record** – and you are now expected to retain and manage every one of those records, for several years or even permanently depending on the nature of the information.
    - The need to manage potentially millions of records each year creates many new challenges for your business, and especially for your IT managers who must come up with rock-solid solutions to securely **store and manage all this data.**

- Let's begin with a look at a few of the SOX sections that call for improved records retention practices.

RECORDS RETENTION IMPLICATIONS OF SECTIONS 302, 404 AND 409

- Sections **302 and 404** have the greatest business impact in terms of ongoing compliance obligations. Section 302 has been in effect since 2002, and Section 404 as of 2004.
    - As companies move from addressing the initial requirements to instituting ongoing compliance efforts, they are turning to technology to ensure better ongoing controls, enforce compliance processes and reduce compliance costs.

Section 302

- Section 302 pertains to **corporate responsibility for financial reports**, and requires that the CFO and CEO personally stand behind the accuracy of their company's quarterly and annual financial statements.
    - To do so, senior management needs to be very confident in the financial documentation that is flowing through the company.
    - In order for the CFO and CEO to certify that the financial statements are 100% correct, systems must be in place to pull together all of the business performance data from all across the company – even if that data resides in various departments, business units, in separate data centers or on different networks.
    - Somehow, toward the end of each quarter, all of the business information must unite into one comprehensive and accurate financial view of the business.'
    - How are financial statements assembled? Typically, all of the divisions and departments within a company submit spreadsheets that roll up the ladder to the corporate accounting or controller's office, where they are further consolidated into a quarterly or annual financial statement awaiting the CFO's sign-off.
    - Several versions of these spreadsheets may flow back and forth as the final numbers are revised, and potentially hundreds of people have input into the final data that will be reported to Wall Street. All of these spreadsheets, as well as all of the documents and emails that were used to arrive at the financial conclusions, are considered records under SOX.

- For example, let's say an accountant in one of your divisions is working to finalize a quarterly financial spreadsheet, and she gets an email at midnight the night before the report is due. The email is from one of her managers, asking her to change a recent sale to Customer X in Singapore from $30 million to $50 million. That email is a business record under Sarbanes-Oxley, and so is every other record in your business that might be used to shape or influence your company's financial reporting.

- It must all be **retained**, and is all **auditable** in the event of any investigation.

- So, before the CFO and CEO sign off on the company's financial statements, they will want to be sure there's a process in place to manage all the records that fed into the financial statements.

- Their name is on the line, and they face severe penalties if serious errors or fraud finds its way into the financial reporting.

- That is why, since SOX took effect, you are seeing an explosion of IT systems that manage documents and records in a very disciplined way, with a clear record of all changes to the data.

- Most large companies have invested in a **centralized document management system** to gain better control of these financial reports, to a much greater level than is possible using spreadsheets. (b)

- We'll talk more about document management systems in the second part of the presentation.

Section 404

- Section 404 requires that **annual reports contain a discussion of the effectiveness of internal controls.** These place major responsibility on the CFO, the company's main compliance gatekeeper. And on the company's external auditors who must provide a public opinion about the reliability and effectiveness of the company's internal controls.

  - What is an internal control? These are not only policies and processes – an internal control may **also include the company's IT systems and records retention technologies.**

  - A lack of good records retention or document management technology might imply a serious lack of reasonable internal controls to an auditor or an investigator.

- SOX does not spell out technology requirements for records retention, but it does clearly imply that companies are expected to exercise strong control over all the records and information that is used to produce financial reports.

- And again, this is not limited to financial spreadsheets in the accounting department. It extends to marketing and sales reports, internal memos, and even instant messaging, and **just about every type of file produced by your employees.**

- We'll take more later about how companies are using technology to control and manage all this huge volume of data, in a way that satisfies the intent of SOX.

Section 409

- Section 409 **mandates significantly expanded disclosure requirements**, with disclosures made as quickly and completely as possible after an event affects the company's performance.

  - Once again, SOX is making a big assumption that companies have almost **real-time visibility** into their company's data, including all sorts of situations and business transactions that are outside the direct control of the accounting or finance functions.

  - For example, let's say that a marketing manager in your European office is made aware that 500 of your company's industrial pumps are about to be recalled due to an engineering defect. The pumps cost $100,000 each. That recall is very likely to have a material affect on the company's financial performance. As soon as the company is aware of this event, SOX requires that it be disclosed publicly, generally **within a matter of a few days**.

  - This has created a demand for more advanced **business intelligence systems** that are actively look across your entire enterprise for events – positive or negative – that may affect your company's financial results.

  - This, too, puts new demands on IT systems and especially the speed of data access.

Sections 103, 801(a) and 802 – the heart of SOX's records retention rules

- Sarbanes-Oxley sections 103, 801(a) and 802 speak directly to **Records Retention.** Section 103 relates to **Audit Work Papers and Evidence.**

  - **Sections 103 (a) and 801 (a)** require public companies and registered public accounting firms to maintain **audit work papers,** documents that form the basis of an audit or review, and all information supporting conclusions for at least 7 years.

- **Section 802** speaks to the retention and destruction of records, with implied penalties.

  - Section 802 **made it a crime** for anyone to intentionally destroy, alter, mutilate, conceal cover up or falsify any records documents or tangible objects that are involved in or could be involved in, a US government investigation or prosecution of any matter, or in a Chapter 11 bankruptcy filing.

  - Section 802 underscores the importance of record retention and destruction policies that affect all of a company's e-mail, e-mail attachments, and documents retained on computers – e-data – as well as hard copies of all company records.

  - The rules states that if you know your company is under investigation, or even suspect that it might be, all document destruction and alteration must stop immediately. And, you must create a company records showing that you've ordered a halt to all automatic e-data destruction practices.

  - Institutions also need to consider all **other regulatory rules** governing records retention with their industry. For example, FFIEC, SEC, IRS, etc…most documents must be retained for 7 years.

  - **Private companies** are also expected to comply with SOX section 802.

  - Private companies now face fines plus up to twenty years imprisonment for knowing destruction, alteration or falsification of records with the intent to impede or influence a federal investigation

SPECIFIC RULES AND BEST PRACTICES FOR RETAINING VARIOUS TYPES OF RECORDS (documents, emails, IM, etc)

- As we've already discussed, the federal government views just about any type of company information as a business record. This certainly includes business documents, in hard copy and electronic form, as well as many other type of electronic files you may not think of as a business record – **but the government does.**

  - **E-data is also subject to disclosure** in lawsuits with non-government opponents in federal and state courts, just like traditional paper documents.

  - Here is just a small sampling of various types of records, and the generally accepted **retention period** for these documents in your systems:

▪ Accounts payable ledger	7 years
▪ Accounts receivable ledger	7 years
▪ Audit reports of accountants	Permanently
▪ Bank statements	7 years
▪ Capital stock and bond records	Permanently
▪ Charts of accounts	Permanently
▪ Contracts and leases	Permanently
▪ Correspondence (legal)	Permanently
▪ Deeds, mortgages, bill of sale	Permanently
▪ Employee payroll records	Permanently
▪ Employment applications	3 years
▪ Inventories of products	7 years
▪ Insurance records	Permanently
▪ Invoices to customers	5 years
▪ Invoices from vendors	5 years
▪ Patents	Permanently
▪ Payroll records and tax returns	7 years
▪ Purchase orders	5 years
▪ Safety records	6 years
▪ Time cards and daily reports	7 years
▪ Training manuals	Permanently
▪ Union agreements	Permanently

  - Of course, there are hundred of other document types that may factor into an investigation or legal action.

  - Such records are assumed to be **searchable and quickly available** upon request, under the rules of SOX. This even applies to less official types of records, like emails or instant messages.

Document Management compliance rules/best practices:

- **Document Management** is essential for implementing centralized storage, archiving and controlled access to documents, as required by Sarbanes-Oxley section 302.

    - If a Document Management System cannot save to a WORM, consider a copy to permanent storage (WORM) and one that is easily searchable on a Document Management System.

    - Data backup of your documents **does not meet** SOX's implied requirement for data archiving, as would be done with a strong document management solution.

    - What's the difference between backup and archiving your records?

    - **Backup** is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. It's usually a routine operation for any organization with valuable data residing on their business computers.

    - Backups are generally performed once per day and capture that data as it exists at the end of each day. There is no requirement for a backup to retain an original copy of the data to be preserved, so the authenticity of the data being backed up in not the primary concern.

    - **An archive is different.** It is a collection of computer files that have been packaged together for backup, to transport to some OTHER location, for saving AWAY from the computer.

    - Archiving creates an exact copy of the data that never changes and is preserved for any number of reasons. This exact copy provides the authenticity to anyone who would need to know that the version of the file is exact.

    - Proper archiving creates a copy of the file each time the file is saved, such that **each version is captured.**

E-mail compliance rules/best practices:

- According to IDC, by the end of this year, the number of e-mails sent annually will exceed nine trillion. For a mid-sized to large company, this can translate into hundreds or gigabytes and even terabytes of email per month.
    - Archiving that volume of email to a compliant WORM-based system with the capability to retrieve specific records on demand requires **a purpose-built records management solution**, designed to scale up as archiving needs grow.
    - In a recent survey on data protection conducted by Enterprise Strategy Group (ESG) 59 percent of enterprise companies and 63 percent of mid-tier companies claim that e-mail is their most critical application.
    - However, e-mail is also becoming the IT manager's worst nightmare, as it relates to compliance.
    - Due to the new regulations, organizations can expect to see e-mail stores increase by 38 percent every year. Simply deleting massive amounts of e-mails to conserve space on your servers is no longer a wise move.
    - Some e-mail management standards and best practices have been established.
    - Four key components to ensure compliance:
        - **1. E-mail must be tamper-proof:** E-mail must be password protected, read-only and non-deletable, encrypted and digitally signed, and exist in a closed system online and offline.
        - **2. E-mail must follow the defined policies of the business:** Policies include what e-mail is archived, how long e-mail archives are retained, and how e-mail is protected.
        - **3. E-mail must have full audit-ability of access and movement**: E-mail must have the ability to be audited by a third party.
        - **4. E-mail must be fully indexed and provide full search capability:** Specifically, e-mail archiving must be index-based on capturing standard RFC-822 header information.

A few keys to compliant e-mail archiving:

- **Discovery:** Information must be easy to access and consistently available in to meet legal discovery challenges from regulatory committees.
- **Legibility**: Information must have the ability to be read today and in the future, regardless of technology.
  - When selecting archiving technology, companies should look for solutions that are based on open systems, in the event that their e-mail application should change. For example, if a company migrates from Microsoft Exchange to Lotus Notes, they must still be able to quickly access and read archived e-mails.
- **Audit-ability**: An email archiving solution must have the ability to allow third parties to review information and validate that it is authentic.
- **Authenticity**: Information must meet all security requirements, account for alteration, and provide an audit trail from origin to disposition. An audit trail can track any changes made to an e-mail.

Technical considerations for e-mail compliance

- The overall e-mail system must include storage devices, and storage arrays; storage networking infrastructure; storage servers; volume management; email archiving or storage backup; email servers; anti-spam and anti-virus systems.
  - Email archive stores are likely to be quite large, so it's worth examining a **variety of storage media**, such as servers or storage area networks.
  - The cost can be high for the equipment and the backup technologies.
  - The cost of managing the stored data is often more expensive than the initial purchase price.
  - The storage system selected must needs to allow for indexing/searching of data, restoration and information retrieval of stored data in a timely fashion. The information's integrity must be maintained. **WORM technology** (or similar) provides that assurance.
- Existing e-mail systems pose a great challenge:
  - Indexing of email is still not fully automated and requires someone to sort it into topical areas, by keywords, metadata, attachments, etc.

- Out of the box, most e-mail systems offer very little for managing content. (d) There are some new technologies being introduced by software companies, promising to make the email indexing process more automated, and screening out all the junk email from the valuable email that companies should retain based on their retention policies.

➢ The industry solution to the email compliance question is to deploy intelligent **E-Mail Management Systems (EMS).**

- These are generally to fulfill regulatory requirements, first and foremost.
- These systems typically index, catalog and record emails based on such information as creator, subject, date or keyword.
- The three most important features companies should look for an Email Management System:
  - are the ability to retain records for a specified period of time
  - the ability to delete records based on corporate or regulatory policy,
  - and search and retrieval capabilities based on specific records or associated content.
- These tools are still new and not widely deployed.
- Research conducted by email management system software vendor C2C claims that 77 percent of companies **still consider backing up their emails as archiving**, and 50 percent of companies are retaining those backups for **only 90 days.**
- So, non-compliance with Sarbanes-Oxley section 802 is probably the norm today.

Likely timeline for evolution of email management systems:

- **2004** – Government regulations continued to evolve and expand encompassing Instant Messaging (IM)
- **2005** – Companies began widespread adoption of archiving as they start to understand their regulatory liability
- **2006** – New technologies enable greater email volume to be stored
- **2006+** - Better archiving and metatagging technologies lead to more viable and affordable systems to automate e-mail management.

Instant Messaging also counts as e-data

- Research shows that if you walk into a typical corporate office, you will find employees using **instant messaging (IM)** on their office PC – and using it for business communications.
    - Surveys by Osterman Research put the penetration of IM to over 90% of all business environments.
    - Nemertes Research found that 74 percent of corporate IM use was initiated by employees using fee public networks, like Yahoo Instant Messenger or AOL.
    - IM is rapidly becoming part of the corporate communications infrastructure – yet up to 90 percent of all corporate use lacks any formal IT control.
    - Gartner Group forecasts that by 2006, more messages will be exchanged over IM than e-mail.
    - But....Sarbanes-Oxley **does not define** any IT requirements for IM compliance and is vague about management and archiving these messages, even if they contain business content.
    - Clearly emails or IMs related to audit work papers and financial controls should be logged and retained for at least 7 years.
    - Other industries, like financial services, have proactively tackled the question of IM compliance.
    - The SEC and NYSE has required that the financial services market treat IM messages **the same as email messages**, ever since 2002.

Steps Toward IM compliance:

- **Assess IM usage** in your company. Since firewalls and other perimeter security devices often fail to block IM use, it helps to implement a network assessment tool that specifically looks for IM activity.
    - There are free tools that can provide a snapshot of IM usage with a minimal investment of IT resources.
- **Develop company policies** for IM use, monitoring and archiving.
    - Compliance requirements, security considerations and business needs can all be addressed in a formal, written policy for IM use.
- **Deploy technologies** to enforce those policies.
    - Limiting IM to authorized users, logging and archiving IM conversations covered by regulations, integrating with email archiving – all can be accomplished with tools now on the market.

RISKS / PENALTIES OF NON-COMPLIANCE

- Failure to follow SOX records retention requirements is now considered an **obstruction of justice** and can result in either fine or imprisonment up to 20 years, or both.
    - If document or e-data destruction continues once you receive a subpoena or request for production in a lawsuit, your legal opponent can ask the court to assess money penalties and other legal sanctions against you for evidence spoliation.
    - There's a great price to pay besides being fined -- Damage to reputation and loss of investor / investment community confidence (share price penalized, increased cost of borrowing)
    - Increase scrutiny of regulators
    - For financial institutions, increased federal deposit insurance premiums
    - Potential business failure: impact on employees, retirees, suppliers and consumers

- One particular public company was being investigated and had 60 days to produce email information, and while they had backups, they were unable to restore and search the data within that time.
    - They had to pay a $10 million fine.
    - The more time passes, the less likely regulators will be to let non-compliant companies slide by without paying fines.

Part II: The Best Practices and Systems to Implement for Fool-Proof Document Retention Under Sarbanes-Oxley

THREE-PART COMPLIANCE STRATEGY

- Your records retention compliance strategy should encompass **three key areas:** Email and IM Archiving and Retrieval; Digital Supervision; Legacy Data Restoration
    - **Email and IM Archiving and Retrieval**
        - A few key features of a strong, **digital archiving solution.**
            - Ability to capture, index, archive, search and instantly retrieve all electronic documents, from e-mail and instant messaging to faxes and online transactions
            - Preserve documents on tamper-proof media, ensuring the highest level on document authenticity, integrity and security
            - A solution that accommodates any unique record retention regulations within your particular industry
    - **2. Digital Supervision**
        - Your **digital supervision system** needs to be able to monitor all employees' electronic communications including e-mail, attachments and instant messages. It also needs to record the supervisory activity and keep auditable records of reviews and other monitoring.
        - Some features to look for in a compliant supervision system include:
            - Efficient review and administration tools

- Ability to index, review and search all electronic communications and attachments
- Ability to flag and annotate selected messages
- A lexicon that can scan email and instant messages to against multiple lexicons of words and phrases; make sure the lexicon is customizeable to your firm's environment.
- A convenient interface that makes it easy for administrators and reviewers to use the system.
- Easily integrates into your existing infrastructure and environment
- Compatible with all major e-mail and instant messaging systems

Legacy Data Restoration

- By converting backup tapes to secure **digital media**, records can be retrieved in a fraction of the time, and at a fraction of the cost, when compared to restoring and searching through backup tapes each time you need a find a record. Some important features for data restoration solution:
  - Automatic de-duplication of data for attorney review – this greatly reduces the burden of producing and reviewing huge volume of records
  - Fully automated restoration process – automation drives down costs.
  - Security and chain of custody – assures that only authorized people have access to your data and tracks their activity with it.

TIPS FOR BUILDING YOUR SOX COMPLIANCE TEAM AND BUDGET

Team Structure

- When drawing up your e-data retention plans, start with Legal and end with IT.
    - Build a **cross-functional team** that includes at least Legal, Finance, IT, Investor Relations and HR.
    - Adding a Corporate Communications representative to the team is also valuable, since all of the compliance policies will need to be **communicated on a regular basis**, in plain language that all employees will understand.
    - Because your compliance plans are likely to require a budget, you may want to **involve the CFO** early in your process, to gain support for the investment.
- Companies that are aggressively working toward Sarbanes-Oxley compliance seem to share certain characteristics:
    - They develop some sort of **roadmap** to guide the activities of personnel who are directly involved in compliance
    - They adopt **dedicated budgets** for compliance management across their organizations.
    - They take a wider view of planning – going beyond financial planning to performance planning. That means having an **enterprise-wide view** of functions and resources, with eye toward connecting every one in the business to one corporate compliance plan.
    - They get their **public accounting firms "blessing"** on your record retention policies before deployment.
    - Through effective communications, they **engage all employees** in the setting of compliance targets.

Team Objectives

- **Consistently enforce** proactive, uniform e-data retention and destruction policies through monitoring and employee education. **Regularly train** your employees on e-data retention policies.

- **Create an inventory** of all electronic hardware and software in use throughout your company, including all cell phones, PDAs, and laptops; all locations and storage formats of archived electronic data; and all methods by which your company's e-data is retained either on premises or in archives, and is destroyed periodically to preserve computer capacities.

- **Create an index** of active and inactive records and implement log books that record when all documents are destroyed. Clearly document that destruction of company e-data is in compliance with consistent retention and destruction policies, and keep those policies updated and enforced.

- **Create a response team** comprised of business, HR, IT and legal staff members. If your company comes under investigation or is party to a lawsuit, that team must be authorized to quickly suspend routine document and e-data destruction companywide, and must communicate to all employees what relevant documents and e-data should be collected and retained.

- **Learn how records retention rules apply to you particular industry**. Some industries like financial services, healthcare, pharmaceuticals, and government agencies have additional layers of records retention rules, above and beyond Sarbanes-Oxley section 802. For example, some government agencies must move their e-mail records to a separate electronic record-keeping system, without the use of backup tapes.

- **Consolidate where possible:** Distributed email servers can send copies of all emails to one centralized email storage system. This gives IT managers one consolidated database of emails, making searches and implementing email compliance faster and simpler.

Budget Planning

- A Gartner Group study last year showed that public companies expected to spend between **$15,000 and $4 million per year** to get in compliance with Sarbanes-Oxley.

    - According to Gartner Research, "a majority of companies **have not** addressed the financial requirements for compliance, spending in an ad hoc fashion to piece together a compliance management process."

IT'S NOT ALL PAIN – SOX COMPLIANCE DELIVERS BUSINESS BENEFITS

Business benefits of records retention compliance

- Biggest benefit is **Risk Avoidance** – avoid an Enron-like disaster
- Sarbanes-Oxley also can be a **lever of change** to overcome past organizational roadblocks to improving information integrity and delivery of timely financial information
- It raises the profile/awareness of **corporate governance**, internal controls and risk management
- It improves the organization's **ability to respond** to changing business circumstances.
- Some of the newer technologies, like business analytics, are initially being bought to help companies comply with Sarbanes-Oxley, though other business benefits will be realized. For example, a strong business analytics solution can **reduce costs** by revealing problems much sooner.
- Building an indexed and searchable e-mail storage system creates a unique **company knowledgebase**. That can have value as an undeletable record of how the company does business, interacts with customers, etc. That is intellectual property which may not exist anywhere else in the company.

Newer compliance technologies promise greater benefits

- Sarbanes-Oxley requires companies to disclose "on a rapid and current basis" and information concerning material changes in their financial condition.
  - According to AMR, 65 percent of large companies are still using manual processes and Excel spread sheets for critical areas of financial reporting and consolidation.
  - While these methods are acceptable in the early years of Sarbanes-Oxley adoption, manual processes and spreadsheets pose serious long-term risks.
  - Spreadsheets spread across an enterprise are not responsive enough to track rapid changes in a company's financial situation, so by the time spreadsheets are updated and moved up the corporate ladder the CFO, a company may already be too late in disclosing a key event to its shareholders.

- This can be viewed as non-compliant with Sarbanes-Oxley.
- Since Sarbanes-Oxley is about reducing the risk of any errors or fraud in the financial statements, companies will be expected to constantly monitor the financial controls of business transactions.
- This is a huge challenge. There are very few business transactions that do not ultimately impact the company's finances, so new systems are coming to market that tie together all of a companies business data.
- For example, if a major customer declines to renew a contract, this decision could have a large impact on a company's earnings, and requires disclosure. Such an event would not normally be detected by the billing or accounting systems until an invoice is generated.
- This could fall outside the company's financial reporting window. To be in compliance with Sarbanes-Oxley, the company would need to recognize and report the material event in something much closer to real time.
- That would call for a system that is almost constantly monitoring all of the company's business transactions, and making those visible to senior management through some type of alerting system.
- This requires a **new breed of business intelligence systems**. Software solutions are now coming to market promising detailed business analytics, to provide continuous, up to date financial visibility.
- The systems are extremely advanced, and aggregate financial information from across the enterprise, even pulling data from systems on very different technology platforms into one cohesive view of the current business situation.
- Once these systems are more commonplace at large companies, they will likely become the expectation of Sarbanes-Oxley compliance, rather than the exception.
- This goes **way beyond records retention,** but I wanted to give you some insights on how Sarbanes-Oxley is driving large and more complex IT changes.

YOUR COMPANY'S NEXT STEPS

- Build a team that brings together internal and external experts and create a **roadmap** for bringing your company into compliance.
    - Ensure that corporate policies are **documented, communicated and enforced** with respect to records retention, reflecting the needs of all legislation in each jurisdiction.
    - Establish a means of **making staff aware** of possible investigative actions, in which case destruction of records may be seen as a criminal act.
    - Records retention is not only, or even primarily, a finance issue. Sales records/contracts, marketing commitments, HR policies, etc. are **all corporate documents** that may be required in an investigative setting.
    - Remember, **electronic media** must also be retained.
    - Meet with your **Internal Audit function** and discuss the requirements of section 404 (annual controls assessment). Objective is to ensure the processes and systems generating financial disclosures are appropriate and provide the necessary assurances for the CEO and CFO to certify the financial statements.
    - Establish processes and technologies that support the ability to **disclose, in real time**, material events, transactions, or other situations that may affect future performance.
    - If you decide to go with a third party for your compliance solution, make sure you choose a company that **specializes in compliance technology,** and has direct, relevant experience working with regulatory issues.
    - Such a partner will have the compliance expertise and know-how to keep your firm safely within industry regulations.

Research Sources:

The Sarbanes-Oxley Act: Taking the CFO's Perspective. IBM Business Consulting Services. 2003.

The Sarbanes-Oxley Act – Business Analytics: Delivering Compliance and Competitive Advantage. Siebel Systems Inc. February 2005.

End-to-End Compliance Solutions: Strategy First. Wall Street Technology. October 2003.

Sarbanes-Oxley: The Competitive Advantage; A Pragmatic Insight into the Issues and Potential Benefits Raised by Sarbanes-Oxley. SSA Global. 2004.

Enterprises Get to Grips with Compliance. Information Week. March 2004.

What Every Company Should Know About Sarbanes-Oxley and Instant Messaging. Akonix. 2004.

Law Creates New Records Retention Requirements. Dallas Business Journal. Mary Ellen Orvis. November 2003.

E-Mail Management – Best Practices for Compliance. ITCI Institute. Steve Kinniston. 2005.

Document Retention Periods. Williams Keepers LLC, Certified Public Accountants. 2005.

www.lighthousecs.com/.../SOX%20Seminar%20Speaking%20Points%20Oct2005%20TMrva.d...