Electronic Records Management Strategies

Presenter: Marty Rehbein, CMC

Member of ARMA International and AIIM

Introduction
Thanks
Survey of attendees
Questions at the end

Electronic records come in a variety of shapes and sizes and are stored in a multitude of ways. Just what are you managing?

- **Video**
- **Cloud computing**
- **Apps, application data**
- **Social media**
- **Smart devices**
- **USBs**
- **Data centers**
- **SANs, LANs, WANs**
- **Computers**
- **E-mails**
- **Software platforms like databases, accounting systems**
- **Websites**
- **Backup tapes**
- **Hosted applications and information**

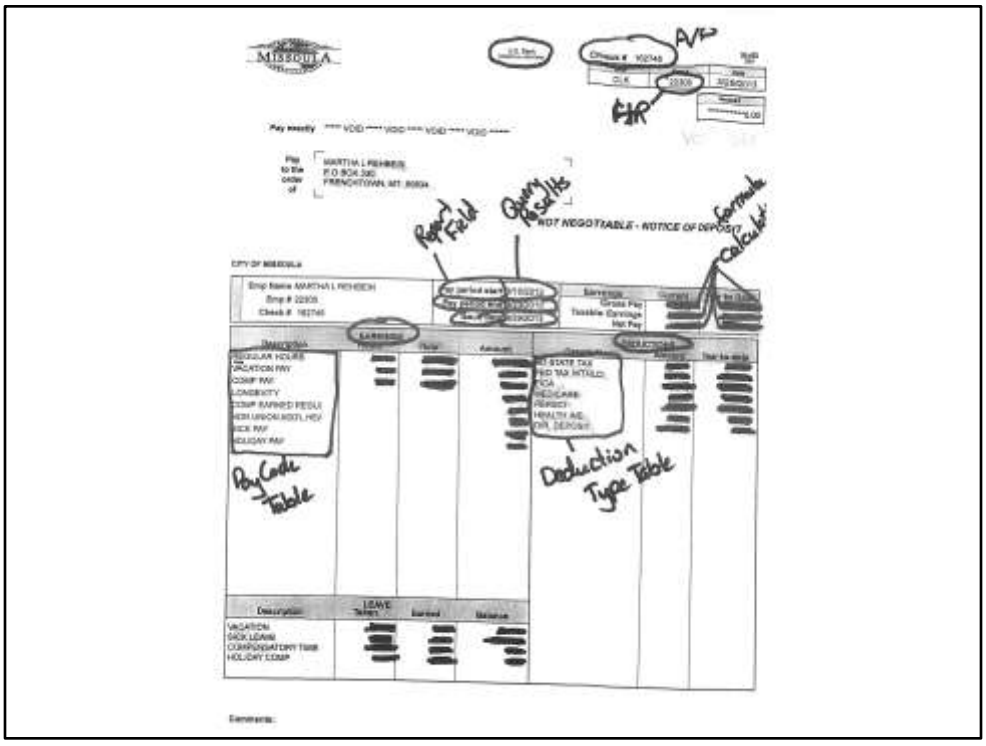
What ARE You Managing?

To err is human—and to blame it on a computer is even more so!

~Robert Orben

Let's not forget people. A system is only as good as the people using it. And remember that people are just trying to do their jobs. Electronic information systems better support them, or they will find a way around "the system" and your attempts to manage it. To do a great job, employees need training on information governance policies and procedures, standards and best practices for managing information related to their jobs and the information system itself. Some common information governance policies include:

- **Records and information management policy**
- **E-communications policy**
- **Internet use policy**
- **Social media policies and guidelines**
- **Security plans**
- **Backup procedures**
- **Employee job handbooks or procedure manuals**
- **Data entry standards**



Here's my paystub. It's comprised of all different fields and tables of information.

This record illustrates how easily an information system can pull together queries, perform calculations pop in a few key fields from data tables and voila! You have a paystub to give your employees every pay day.

This record also illustrates some of the difficulties associated with electronic records. You see throughout my 22 year career, information on this record has changed.

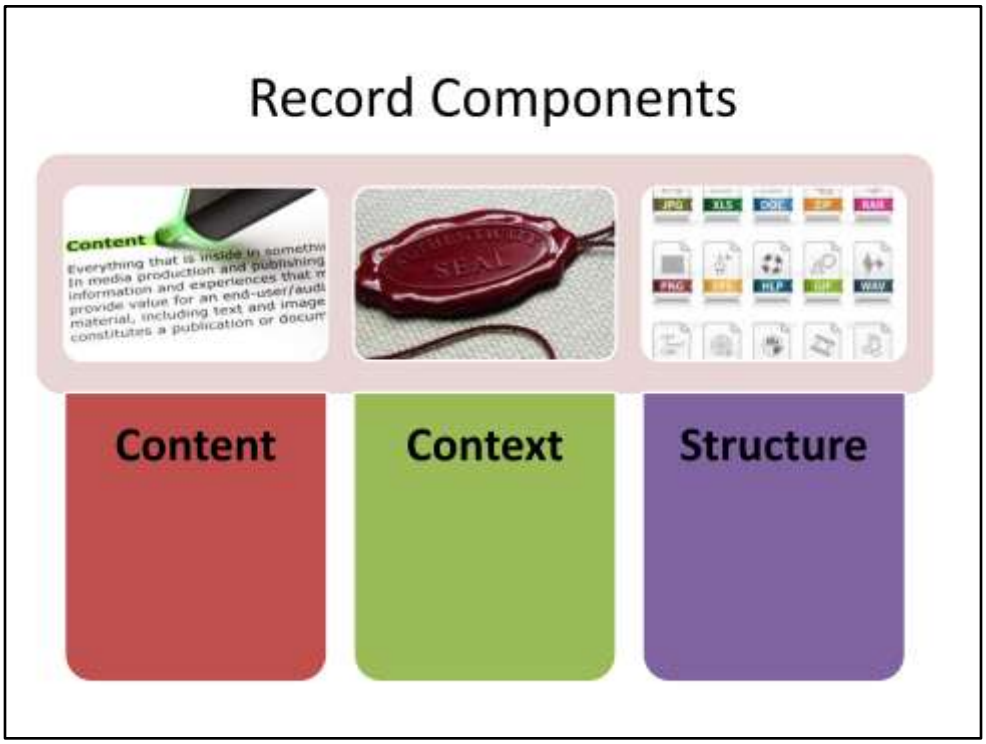
- **My name and address changed.**
- **Withholding formulas have changed**
- **My rate of pay has changed**
- **The amount of vacation I accrue has increased**
- **Etc.**
- **Given all these changes, if the city had to, could it produce the amount of the first contribution I made to PERS in my first pay check back in 1991? Electronically no. We've switched software since then. Paper, yes, there is a payroll report our payroll clerk printed out on green bar paper in a great big binder.**

Electronic Records

Electronic records are not human readable, so they require special management.

Their physical appearance along does not provide sufficient information to determine their origin, purpose, or other aspects of the context in which they were created or maintained.

Maintaining an electronic record's content, structure and context is essential to success!

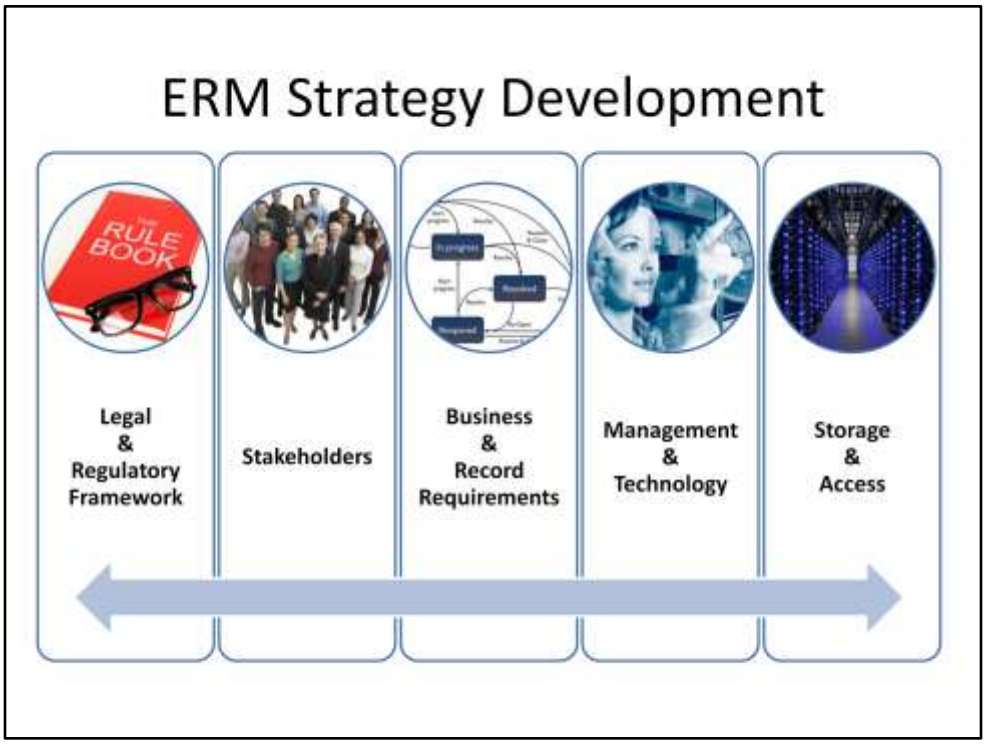


So let's look at those components a little more closely.
***Content* is the substance of the record. It's the text, data symbols, numbers, pictures, images and sound.**

Examples: E-mail message body, report data, pictures of an accident, voice mail audio files, video of students on the bus

***Context*. Information that show how the record is related to the business of the district and other records.**
Examples: Metadata like e-mail message headers, routing/approval history, author, last edited/modified/printed information usually found in document properties

***Structure*. Appearance and arrangement of the content**
Examples: File name, file format, fonts, formatting, page breaks, hyperlinks, e-mail attachments, colors



When you begin to develop your electronic records management strategy, you should aim for a policy that integrates:

- **The legal and regulatory framework of your district**
- **The interests of your stakeholders (e.g., staff, faculty, students, board of trustees, citizens, regulators)**
- **Your business and electronic record requirements**
- **Management policies for people and technologies**
- **Long-term storage and access needs (both legal and operational)**

A sound, integrated strategy reflects the relationship between records and information management and your operations, and ensures that you manage records in a way that supports your daily work, supports long-term operational needs, and meets your legal requirements.

Because different stakeholders throughout an enterprise have different needs and roles in electronic records management, the development of your electronic records management strategy requires joint planning, communication, and training.

In the paper world, staff create records and process them. When it's time to store them, the records are put in a labeled box and placed on a shelf to wait until they can be disposed.

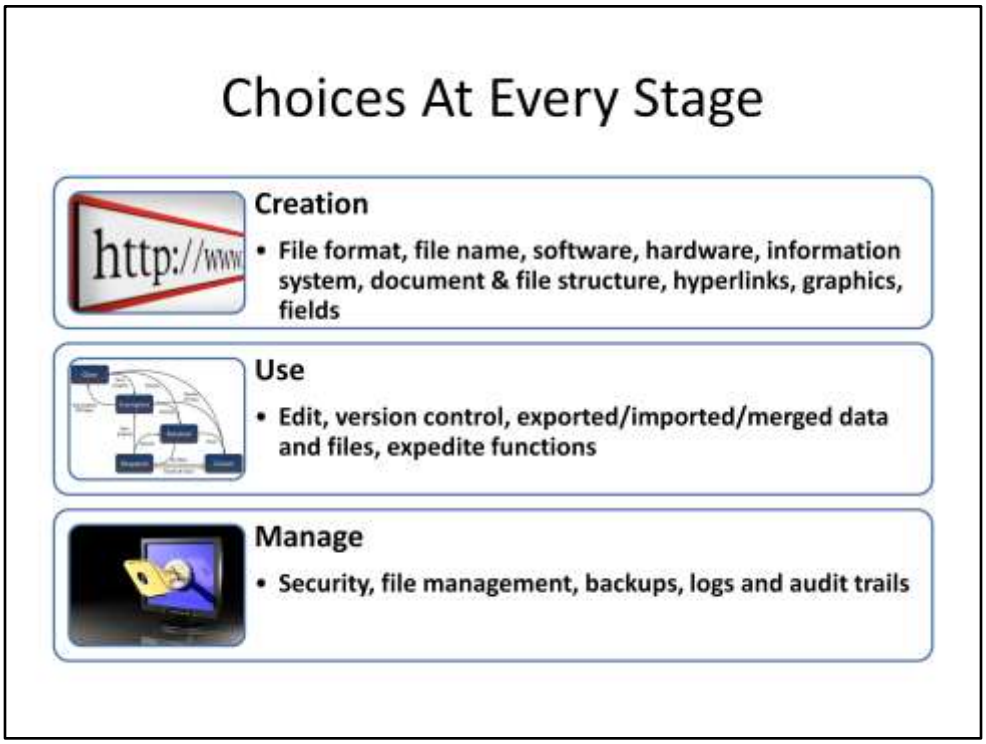
Electronic records don't work that way. When you and your staff create, use, manage, retain and dispose records you make choices that affect your ability to do your work as well as store records and information through its retention period. In short, begin with the end in mind. Be intentional about the creation and management of electronic records.

Some common issues with electronic records:
How many of you have had a hard drive failure and lost all your files?
Have you ever not been able to find an electronic file you need?
Have you ever bought a new information system to replace your old one? What did you do with the information and records on the old system? Did the transition go smoothly?
Have you ever received a discovery request in a lawsuit for all e-mails relating to X?
Have you or someone you know ever been hacked?
Have you ever had difficulty ascertaining the latest version of a document?
Do you have an "F" drive that is cluttered with "stuff" that you aren't sure about?
Do people in your organization have mobile phones or laptops that they use away from the office for business?

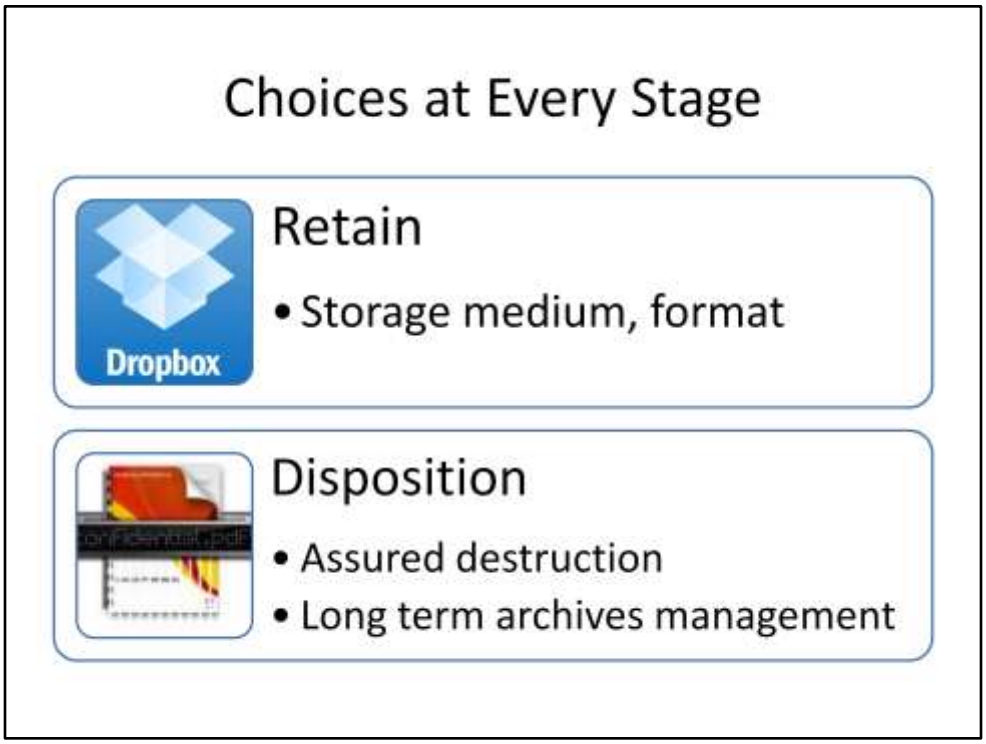
Has anyone ever lost or broken a phone or laptop? Do you have any idea what information was on it?
What happens to an employee's e-mail when they leave your organization?

A successful ERM strategy reflects the records management continuum or lifecycle and addresses these questions.

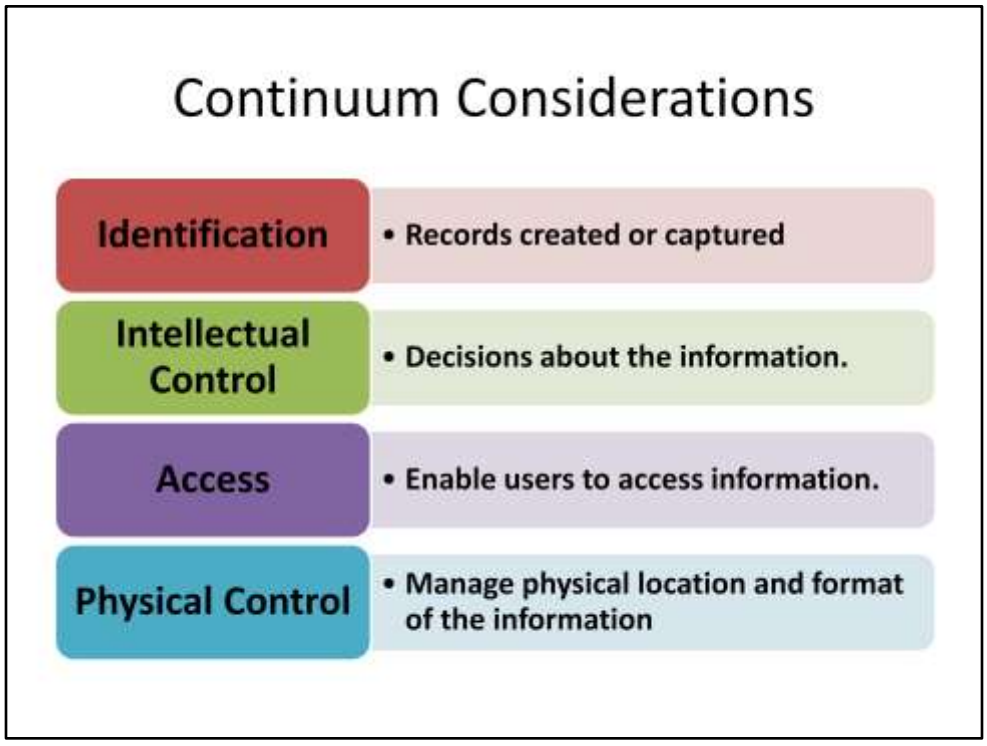
Let's talk about some of the choices you make at each stage:
Creation—File format, file name, software, hardware, information system used, file structure, hyperlinks, graphics
Use—Edit, Version control, exported/imported/merged data
Manage—Security, file management, backups, log files
Retain—Storage medium, format
Disposition—Assured destruction, long term archives management



Let's talk about some of the choices you make at each stage:
Creation—File format, file name, software, hardware, information system used, file structure, hyperlinks, graphics
Use—Edit, version control, exported/imported/merged data
Manage—Security, file management, backups, log files
Retain—Storage medium, format
Disposition—Assured destruction, long term archives management



Retain—Storage medium, format
Disposition—Assured destruction of all copies, long term archives management



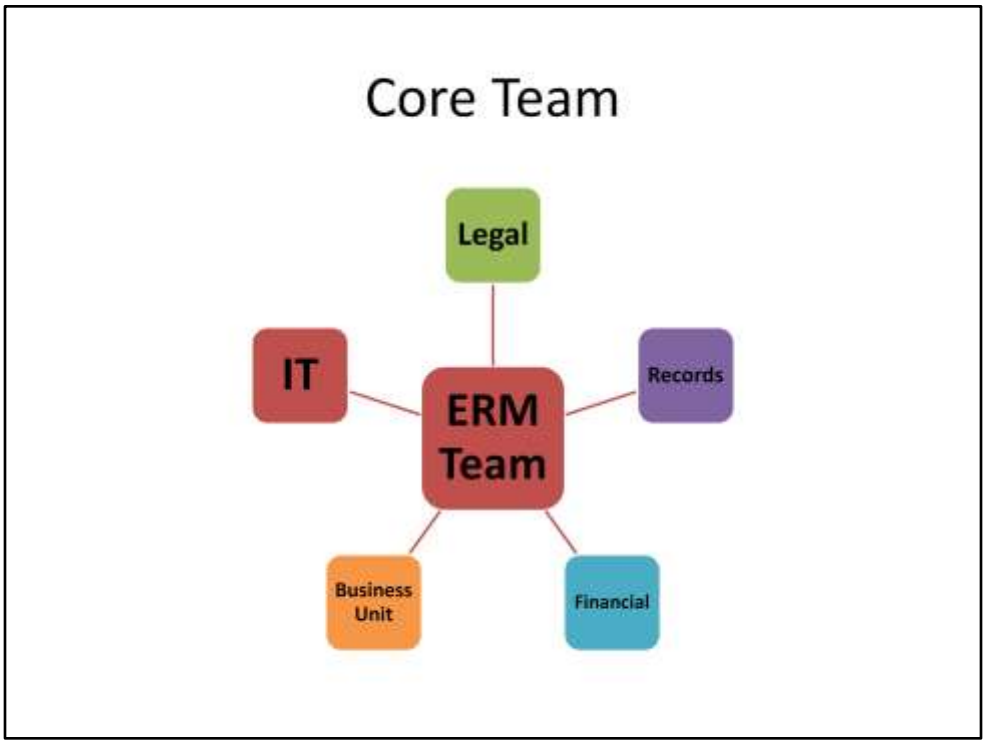
There are four actions that recur throughout the continuum of information and records.

Identification:
What points along the business process do we receive records or need to create or capture records?

Intellectual Control:
What can happen to the information? Who makes the decisions about the information? Who can change security, work flows, forms? Who decides what records must moved off of the old system?

Access:
Who can look at the information? Can it be released to the public?
Who can create, change, approve, review, reassign, print, delete information on the system?

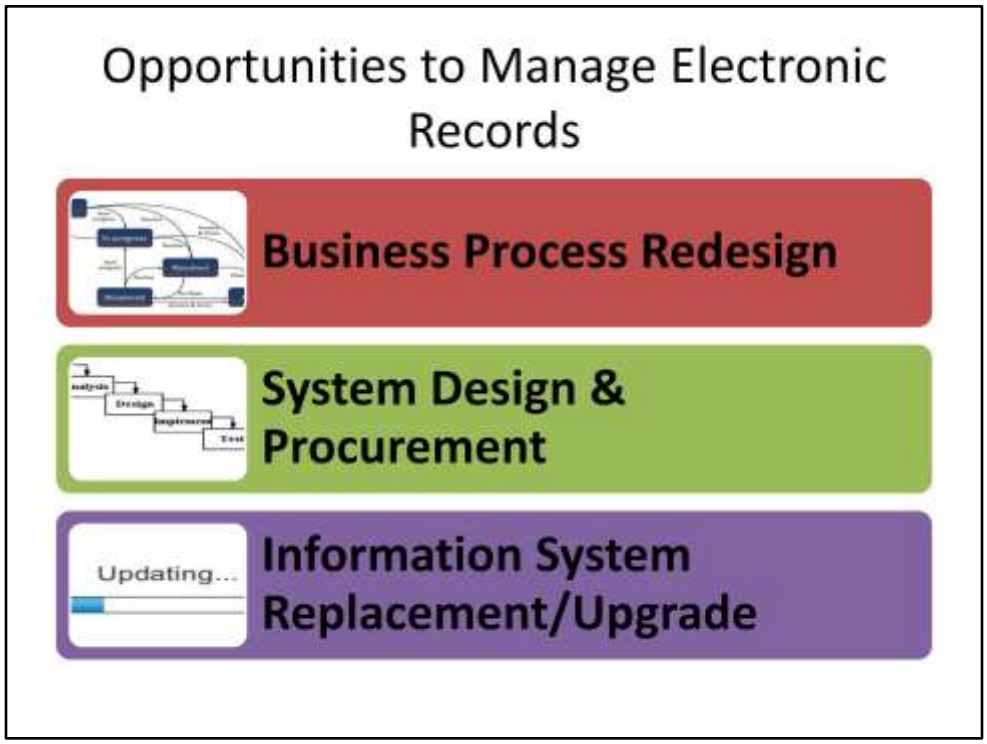
Control: Who determines where the records are stored and what format is selected?



You should include the following disciplines from your organization on your ERM team:

- **Legal—laws and rules**
- **Records Management—records retention schedules, structuring information**
- **IT—technical expertise**
- **Business unit—business process knowledge**
- **Financial—knows audit requirements, financial support, knowledge about transactions**

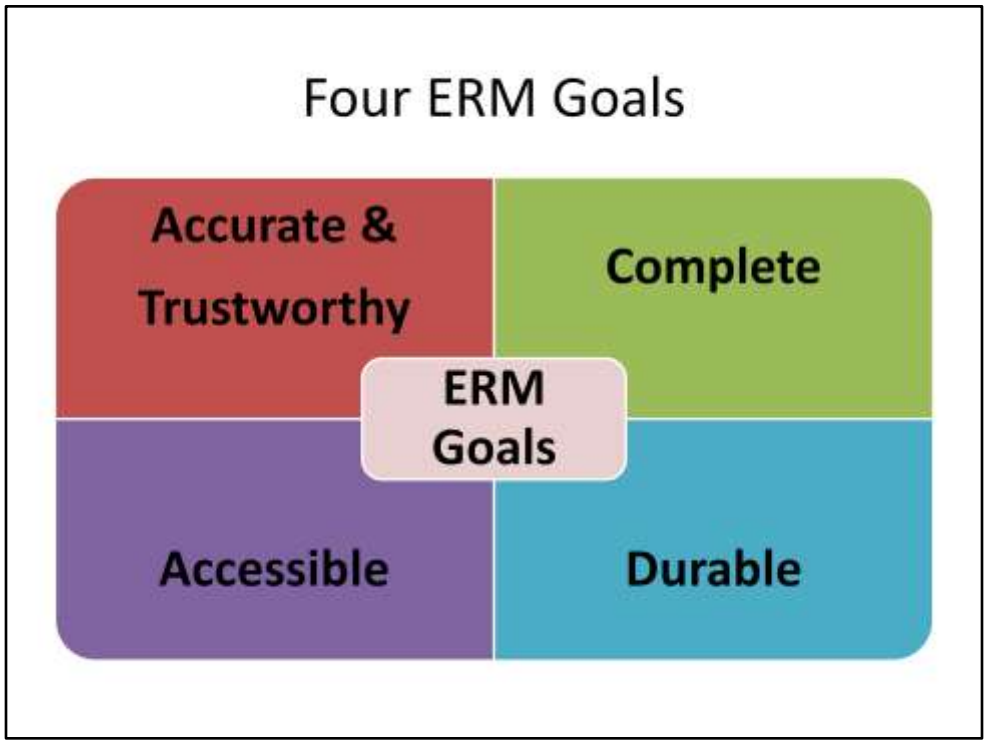
Yes, you can add additional team members if they have expertise you need.



Business process analysis and reengineering are powerful tools that organizations are using to streamline their processes, eliminate redundant tasks and improve efficiency. Process analysis and redesign are excellent opportunities to also reconsider recordkeeping practices, since they often identify problems which could be alleviated through new workflow procedures and/or information systems. If recordkeeping requirements are identified during process analysis, effective procedures and automated routines can be built into the revised processes to handle records more effectively.

Another opportunity is when you are designing and procuring a new system. A new system may automate manual processes or automate information handling or reporting requirements.

Another great opportunity to gain greater management over electronic records is when you upgrade or replace an information system. This is an opportunity to address pain points staff had with an old system including data entry standards, more robust searching functions, enhanced security, version control features. It's also important to consider your legacy records and information on the old system.



Trustworthy electronic records contain information that is reliable and authentic. A key aspect to trustworthiness is legal admissibility, i.e., whether your records will be accepted as evidence in court. Will they pass muster with your auditors or meet your legal and regulatory obligations?

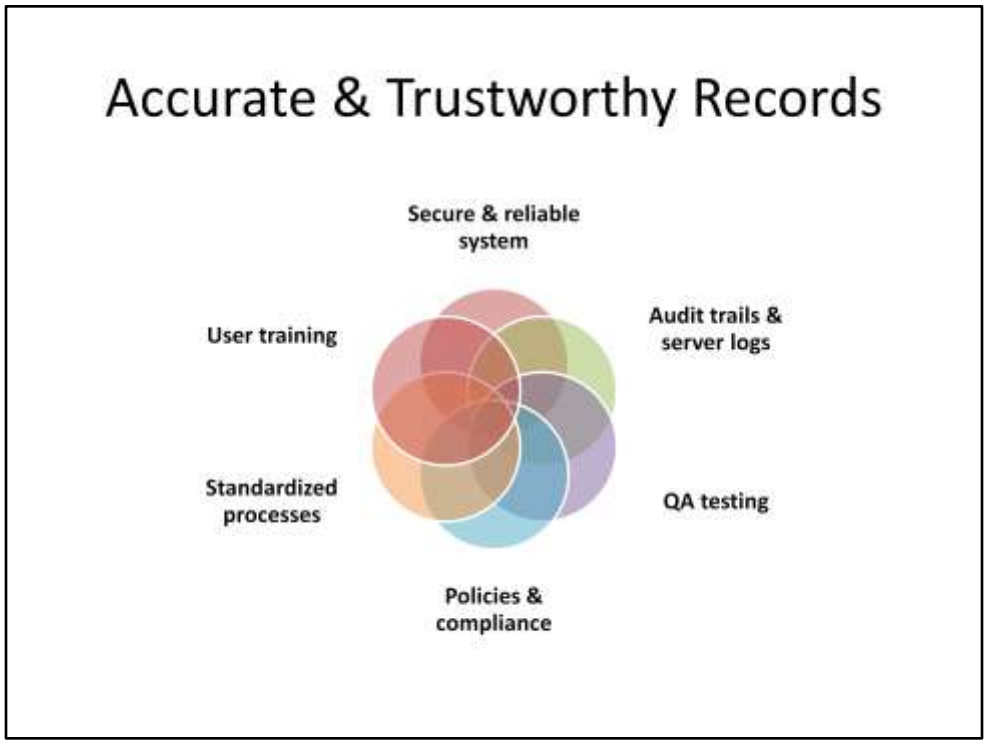
Your records should be complete and unaltered through tampering or corruption. They should have all the information necessary to ensure their long-term usefulness including their content, context and structure.

You will also need to capture and maintain the necessary metadata about your records. *Metadata* is the "data about the data" that documents the relationship of the record to your business process and to other records. Metadata ensures that you can find and use your records. Metadata can include elements like the record's creator, the date of creation, the file name, size and type, when the record was last modified, the business unit the record is associated with, and the record series to which the record belongs.

You should be able to locate and access your records in a way that meets your needs and the needs of your stakeholders. Some records may need to be immediately accessible, while others may not.

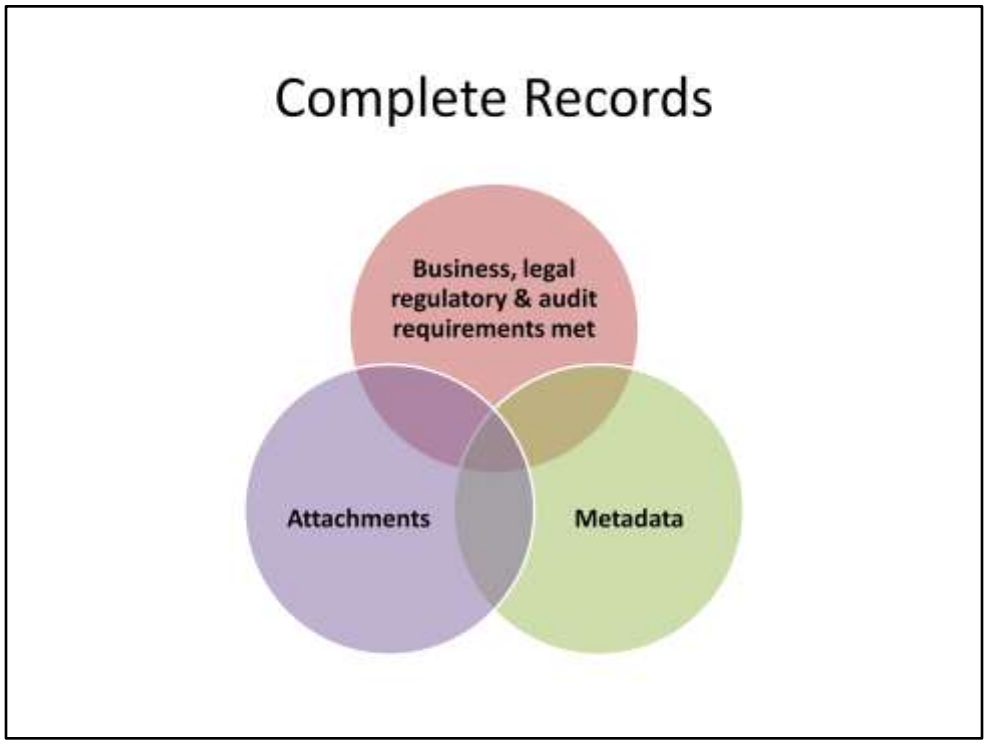
You also want to ensure that your records are durable. In other words, they must be

accessible for the designated records retention period and stored appropriately. It also means you need to safeguard electronic records and systems in the event of a disaster, so you can resume business.



So how do establish the accuracy, integrity and trustworthiness of your electronic records?

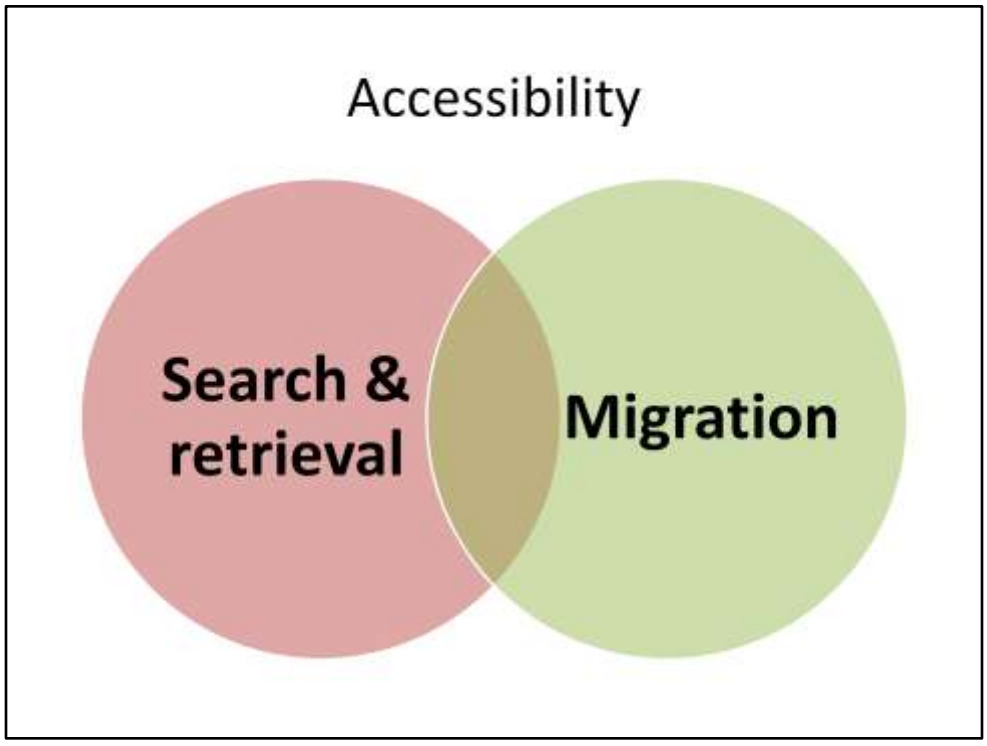
- **The information and the systems used to manage it should be secure and reliable.**
- **The system should provide audit trails, tracking systems and server logs that are sufficient to demonstrate the reliability of both the system and the information it contains.**
- **There should be regular quality assurance testing for the system software and hardware, processes performed by the system, information stored in the system, and business continuity plans associated with the system and the information.**
- **Written policies about information systems and the personnel using them are reviewed regularly for consistency with current practice. Policies are followed consistently**
- **Processes and procedures associated with the system are standardized and documented**
- **System users receive consistent, documented training.**



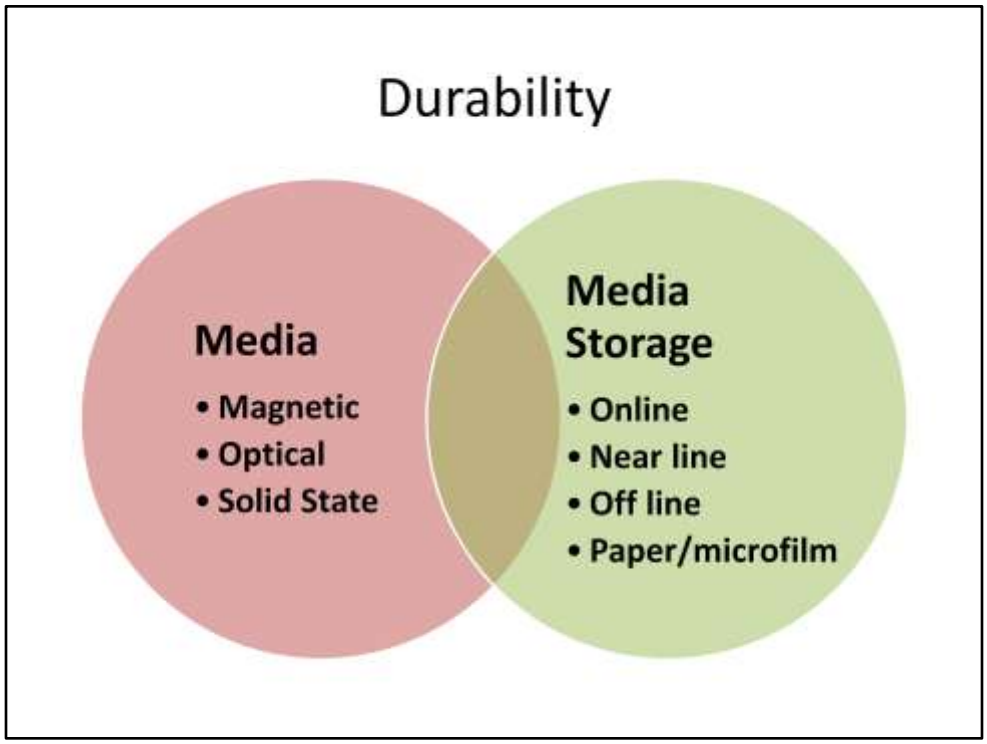
Complete records have all the information necessary to ensure their long-term usefulness and accessibility. They document key points of a business process, demonstrate that you have met legal, regulatory and audit requirements.

Complete records include necessary metadata about the records. Metadata ensures you can continue to find and use your records, sometimes even long after the system that created them has been replaced or rendered obsolete. It includes things like author, key dates—created, modified, accessed, printed, file type and size, file location, etc.

Finally, don't forget about attachments. Images and files uploaded to databases and websites, e-mail attachments, etc. Sometimes the attachments are more important than the record. Think about an e-mail with only the text, "Please proceed with the work outlined in the attached memo."



Records should be easily retrievable in the normal course of business during their lifecycle. Many systems provide robust search and retrieval functions to help you find information quickly. Think past your current system. When you get a new system, you will eventually replace it. Think about designing the system so you can easily migrate content to the next new system. Trust me, your vendors aren't probably going to prompt you to think about the day when you might leave their product behind!



There are many options to store your information. Be intentional as you select the media and its storage location because all media and storage solutions will meet your business, legal and regulatory requirements.

There are 3 types of digital media:

Magnetic media includes things like backup tapes, some hard drives and network servers
Optical media include CDs and DVDs
Solid state media include USB flash drives, some hard drives, and flash memory cards

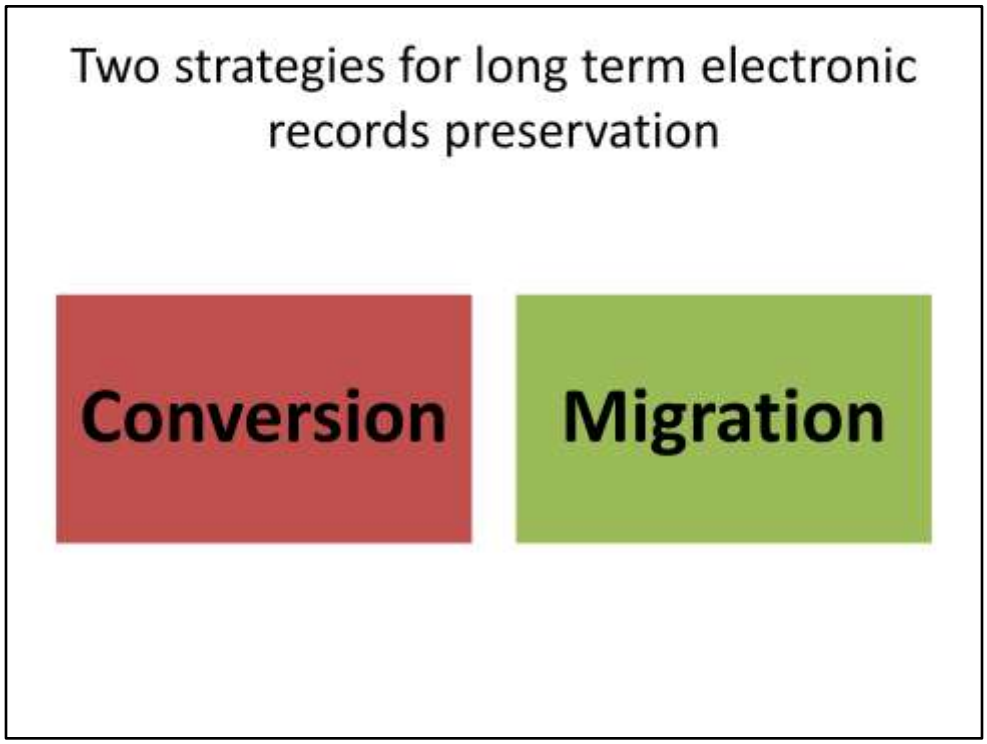
All digital media have a finite life span which are dependent on a number of factors, including manufacturing quality, age and condition before recording, handling and maintenance, frequency of access, and storage conditions. Studies have indicated that under optimal conditions, the life expectancy of magnetic media ranges from 10 to 20 years for different types, while optical media may last as long as 30 years. However, in real life situations, most media life expectancies are significantly less.

You also have choices about where you store information including:

Online—Information is stored online and is continually accessible. This option maintains the greatest functionality but requires more expense to maintain

Near line—Information is stored on a removable media like a disk or a SAN array. Generally they are still accessible via the network. This option maintains a moderate amount of functionality. Storage space is less expensive than online storage.

Offline—Information is stored offline on removable media that is not accessible through a network. This option trades functionality for stability.



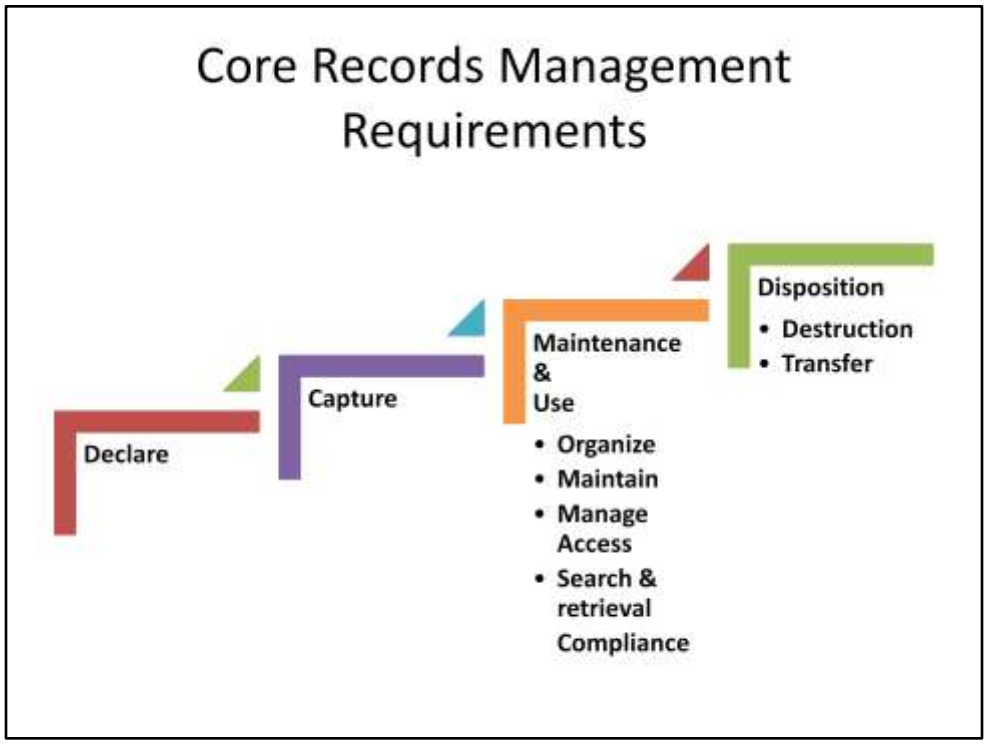
You have two viable, often compatible, approaches for the long-term retention of your records:

***Conversion*. When you convert a record, you change its file format. Often, conversion takes place to make the record software independent and available in an open or standard format. For example, you can convert a record created in Microsoft Word by saving it as an XMT, PDF or RTF document. Be intentional about the file format you select because it will affect the durability of your records and information. Non-proprietary file formats and software platforms with open standards are best.**

***Migration*. When you migrate a record, you move it from one computer platform, storage medium, or physical format to another. For example, you may move your legacy records from your old system to your new one.**

You will be faced three basic types of loss when converting or migrating files that will need to be considered before finalizing your plan. The amount and type of loss needs to be analyzed to determine the best course of action. The three types of loss are:
Data. If you lose data or if it becomes corrupted, you lose, to a varying degree, the content of the record. Bear in mind that, legally, your records must be complete and trustworthy. Metadata may also be altered or lost.
Appearance. If you convert all word processing documents to RTF, you risk loss of the structure of the record; you may lose some of the page layout. You must determine if

this loss affects the completeness of the record. If the structure is essential to understanding the record, this loss may be unacceptable.
Relationships. Another risk is the loss of the relationships of the data within the file or between files (e.g., spreadsheet cell formulas, database file fields). Again, this loss may affect the legal requirement for complete records.



As you implement a system, you'll have a long list of business and system requirements. Here are the core records management requirements you can build specifications around:

Declare—Recognize when a record is or should be created
Capture—Include a record in the system
Maintenance & Use

- **Organize—group information according to a predefined structure**
- **Maintain—protect the integrity of records against unauthorized alteration or destruction**
- **Manage access—grant or limit the ability of individuals to examine information**
- **Facilitate retrieval—provide or enable the ability to collect records relevant to a query**
- **Preserve records—ensure you can still render and read your information so it remains useful**
- **Compliance—ensure compliance with laws, regulations, policies, standards and procedures.**

Disposition—the final resting place for information

- **Destruction—eliminate records and information from a system in compliance with your records retention schedule so they cannot be accessed, retrieved or recovered**
- **Transfer—change the legal custodian of the records to another entity**

Let's run e-mail software through this list and see what we come up with.

Does the software help you identify records that might be created using e-mail?
No. A e-mail accepting placing an order for office supplies and a lunch invitation use the same format.

Does the software allow you to capture e-mail records?
Yes. In fact, e-mail is so good at capturing records and other extraneous stuff it is a treasure trove for attorneys

Does e-mail software allow you to organize information?
Yes. The structure outside of To; From; and Date: is up to individuals though.

Are there good security measures available with your e-mail software?
Generally yes until you're hacked.

Does e-mail software provide search and retrieval capability?
Yes and no. You can sort, filter and search your messages quite easily. But it falls down if you have to respond to a broad discovery request for a lawsuit or public records request? E-mail can be forwarded, printed, BCC'd. Multiple files of archived mail can be saved on servers, hard drives. It's on mobile devices.

Does e-mail software enable you to preserve messages so you can render and read them?
Yes. If you migrate to a new e-mail platform, you might have a few surprises though.

Does your e-mail software enable you to tell if people are complying with your policies?
No. E-mail can be used to harass or create a hostile work environment.

Does your e-mail software enable you to delete messages in accordance with your retentions schedule?
No. How will you ever know if you've deleted every copy of a message to comply with your retention schedule?

Does this mean we shouldn't use e-mail?
No. It's just an example of a widely used system that doesn't dot the T's and cross the I's when it comes to Records Management. You've probably already bought additional tools to address some of your pain points with e-mail.

You probably have:

Spam and virus filters
Acceptable use policies

You might have:
Centralized folders for your staff
E-mail archive solution
Retention management solution

Questions?

Slides with notes will be available on MASBO website