Ensuring Digital Continuity
What's Your Plan?

National Association for Court Management
2015 Annual Conference

Nial Raaen, CRM
NCSC Principal Consultant

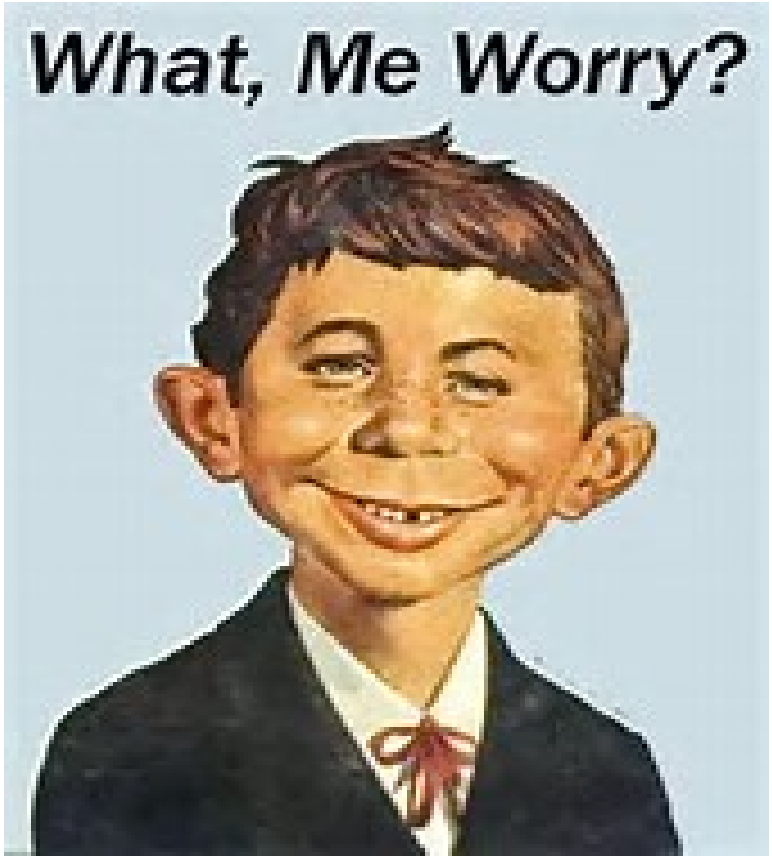
National Center for State Courts

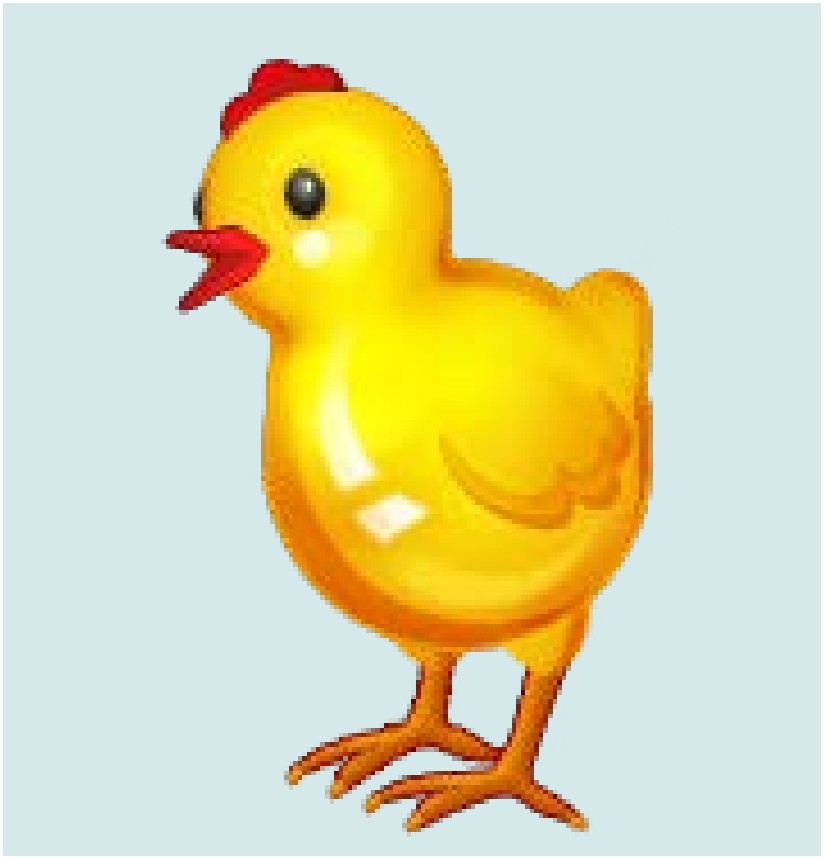
What is Digital Continuity?

Keeping and managing digital information to ensure it can be used in the way that is required, for as long as required, *and no longer*.

DIGITAL CONTINUITY PLANNING

Alfred E. Neuman or Chicken Little?



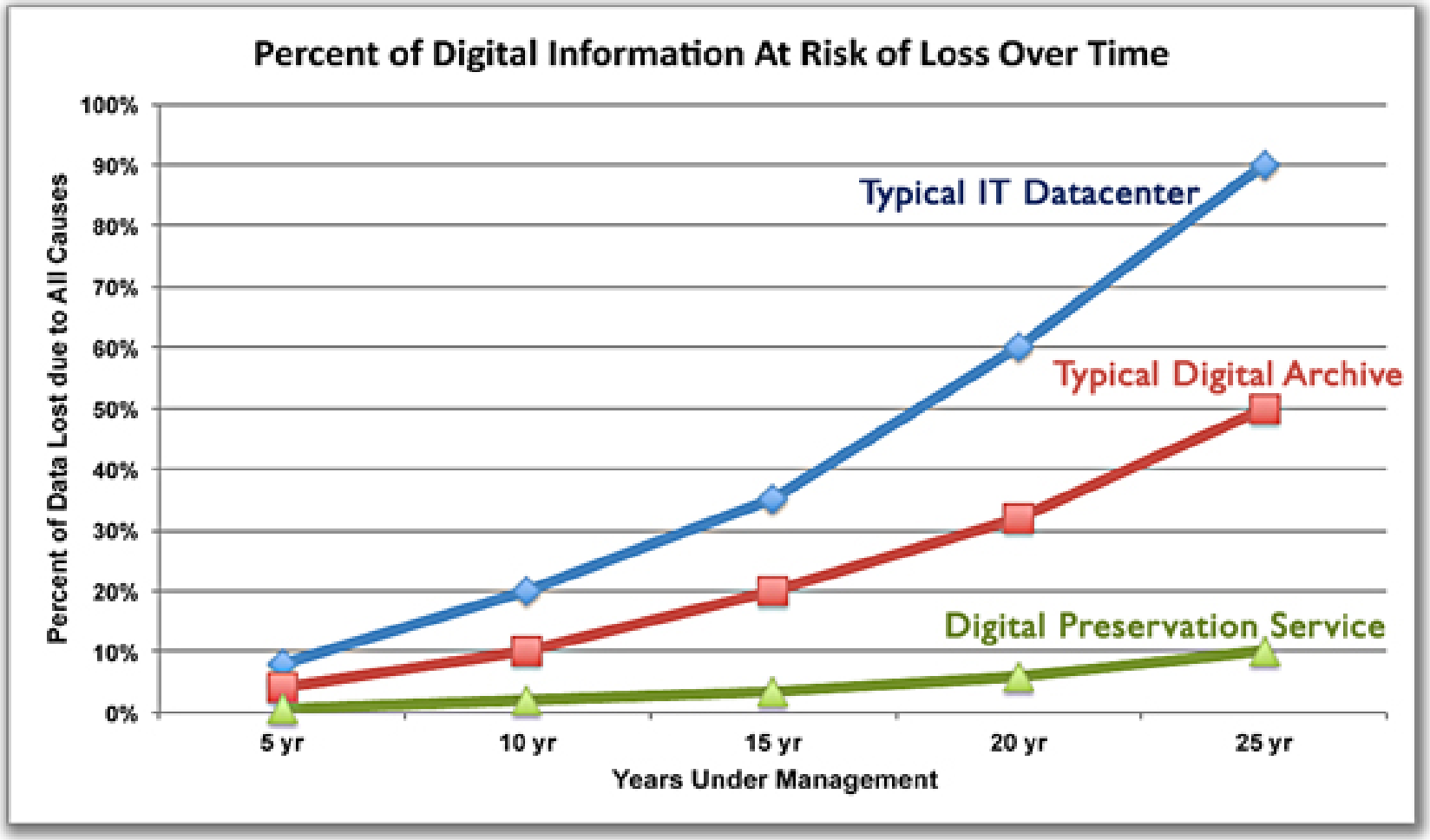


The Challenges…

- Increasing reliance on digital systems as e-filing and EDMSs are adopted, records are “born digital”
- Rapid technological change and technical skills
- Complexity of ER retention and disposition
- Planning and collaboration are more critical

No universal solution exists today for permanent or long-term digital preservation

Which Future?



Source: The Long-Term Digital Preservation Reference Model, www.ltdprm.org 2012

Digital Record Risk Factors

Risk of Loss or Alteration Increases with…

- **Time**
- **Frequency of access**
- **Complexity of the material**
- **Volume of records**

Electronic record keeping systems are inherently more vulnerable to alteration, loss or disclosure

Knowledge is Power

- Know What You Have
- Know Your Capabilities
- Know Your Options
- Know Your Vulnerabilities
- Know When to Say Good-Bye

What's on Your Server?

Know what you have

- Content and formats
- Anticipated changes to systems
- Retention requirements
- Record value
- "Unofficial" records and systems
- Unstructured records

“Unstructured” Records

Office automation work products

- Documents
- Spreadsheets
- Presentations

Social media

Web content

Email

Managing Email

Over 130 billion emails sent & received *per day* *but*,

- When is it a record?
- Retention depends on content and context
- Classification systems can help
  - Automated
  - Manual
- More than 85% of emails may be “transitory”

“Open” Formats

- TIFF
- XML
- JPEG
- PDF/A

Record Surveys and Inventories

Records Survey – identifies broad series or classes of records, to assess care and organization, volume, storage media, and record formats

Records Inventory – detailed analysis of specific types, quantities and conditions of records to assess systems and compliance with policies

Know Your Capabilities

Are you "preservation ready"?

- Technical expertise
  - Local staff and vendors
- Governance
  - Clear accountability and roles
  - Funding (5 years +)
  - Collaboration
- Technical systems and standards

Self-Assessment Tools

- Digital Preservation Capability Maturity Model and Checklist
- National Digital Stewardship Alliance Digital Preservation Framework
- NCSC Judicial Records Maturity Model

Know Your Options

Determine the best strategy based on:

- available technology
- the type of records and their lifecycle
- storage systems

Watch for emerging technologies

- be cautious with adoption

Learn from the records management community

Preservation Strategies

Media obsolescence

- Copy records to current media while the legacy media and readers are still available
- Choose common, market-accepted media

Preservation Strategies

Media degradation

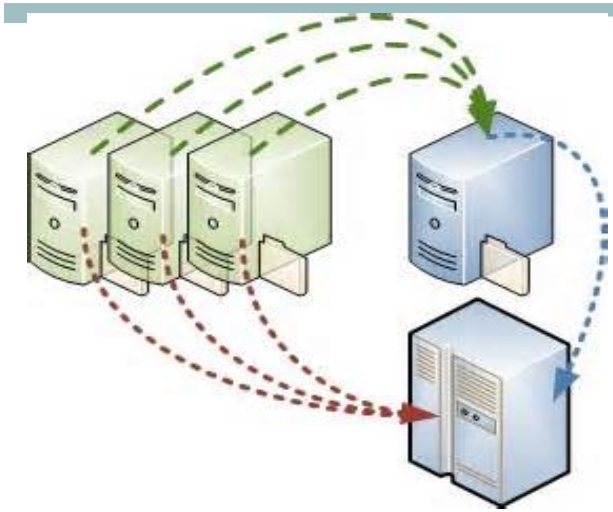
- Choose high-quality or archival media
- Store in a controlled environment
- Protect media from damage
- Maintain redundant copies

Preservation Strategies

Format obsolescence

- *Technology preservation* – a short-term solution
- *Emulation* – a short to medium-term solution
- *Migration* – the **most effective** solution available

Migration



An active preservation strategy

- Cycle is approximately every 10-15 years
- Media and file types must provide a stable repository for preservation and access
- A migration strategy and schedule should be established for specific media and file types

Migration Approaches

NORMALIZATION or “migration on ingest” is transferring records to a digital storage repository in an open source format

MIGRATION AT OBSOLESCENSE – or “just in time” is migration dictated by impending technological obsolescence

Storage Concepts

Storage refers to the media where data is stored to meet daily business requirements.

Backups are copies of operational data that can be used to restore files, system data, or an application to its original operational state.

Archives are records selected for permanent or long-term preservation.

Magnetic Tape

- Most common backup media
- Fast write but slower read
- High capacity per media
- Some are WORM, majority rewritable
- Lifespan of 5-10 years (?) 30(?)

Optical Disk

- Uses laser technology to write to media
- Relatively slow to write to and read from
- Limited storage capacities per media compared to magnetic disk or tape
- Lifespan of 10-50 years
- Includes WORM disks, CDs, DVDs

Solid State (SSD)

- Transistor-based storage includes solid-state disks (SSD), USB flash drives
- Relatively new to the storage market
- Fast read and write speeds
- Lower storage capacity to date than magnetic or tape, but higher than optical
- Inherently rewritable
- Lifespan TBD

Personal Storage

- Wide variety of devices and capacities
  (flash drives, MP3 players, smart phones, laptops, external disks)
- Most useful for transport and backup
- Generally limited storage capacities
- Difficult to control or monitor
- Susceptible to loss or theft

Cloud Technology

Advantages:

- Shared cost
- Quick startup
- Shared resources
- Scalable to need

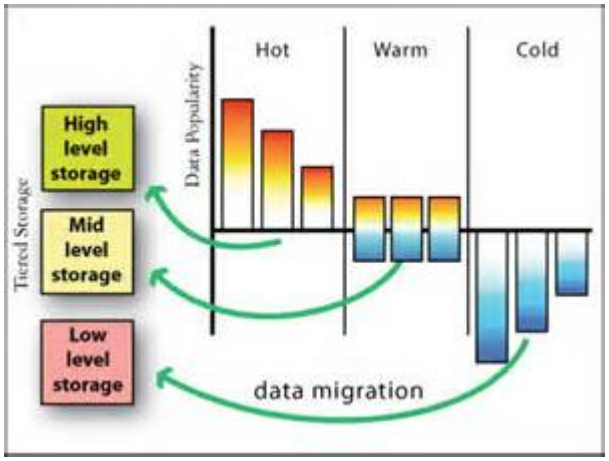
Concerns:

- Security
- Ownership
- Access
- Vendor viability

Information Lifecycle Management Approach

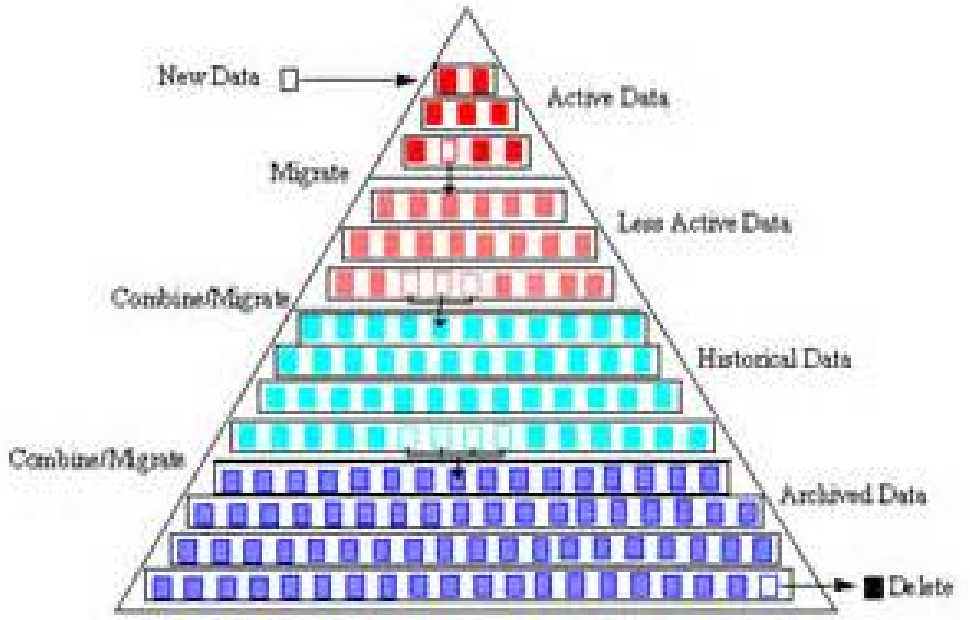
- Tiered storage solution uses one or more of the types of storage
- Uses the context of information to assign it to different storage tiers
- Different tiers use different media, backup and recovery modes

Tiered Storage



Based on:

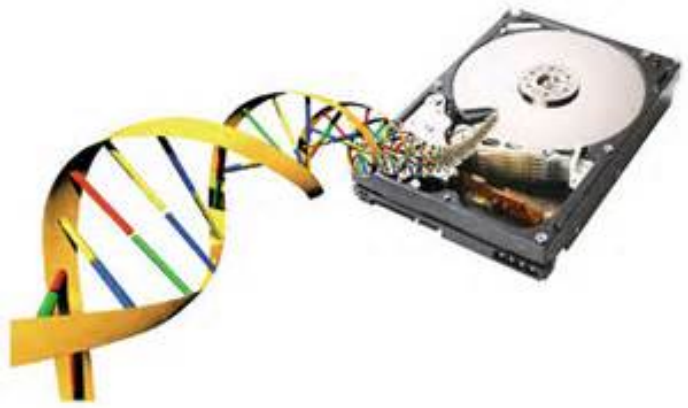
- Availability
- Performance
- Recovery



Storage Technology Selection

- Access requirements (speed and frequency)
- Media lifespan
- Hardware compatibility over lifespan
- Lifecycle management requirements
- Technical capacity and capabilities of staff
- Cost of acquisition and maintenance
- Consider total record lifecycle needs

News Flash!

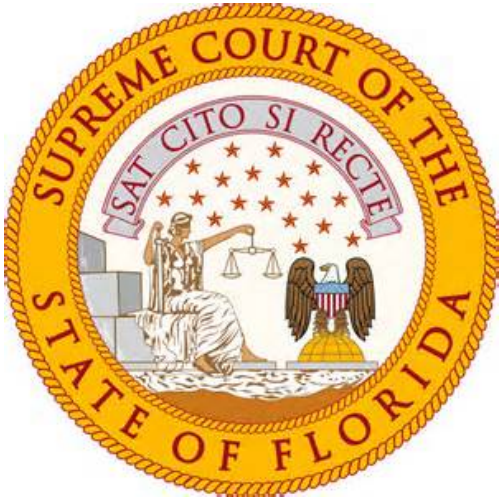


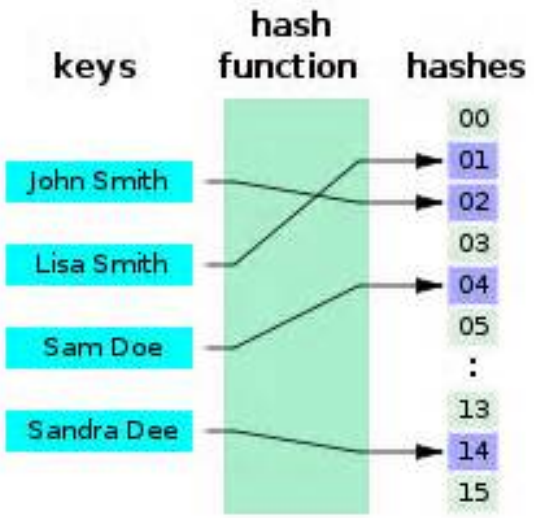
Scientists at Harvard's Wyss Institute were recently able to store nearly 700 terabytes of data in a single gram of DNA, 1,000 times greater density than previous attempts.

Know Your Vulnerabilities

Maintaining Authenticity and Integrity

the old and the new



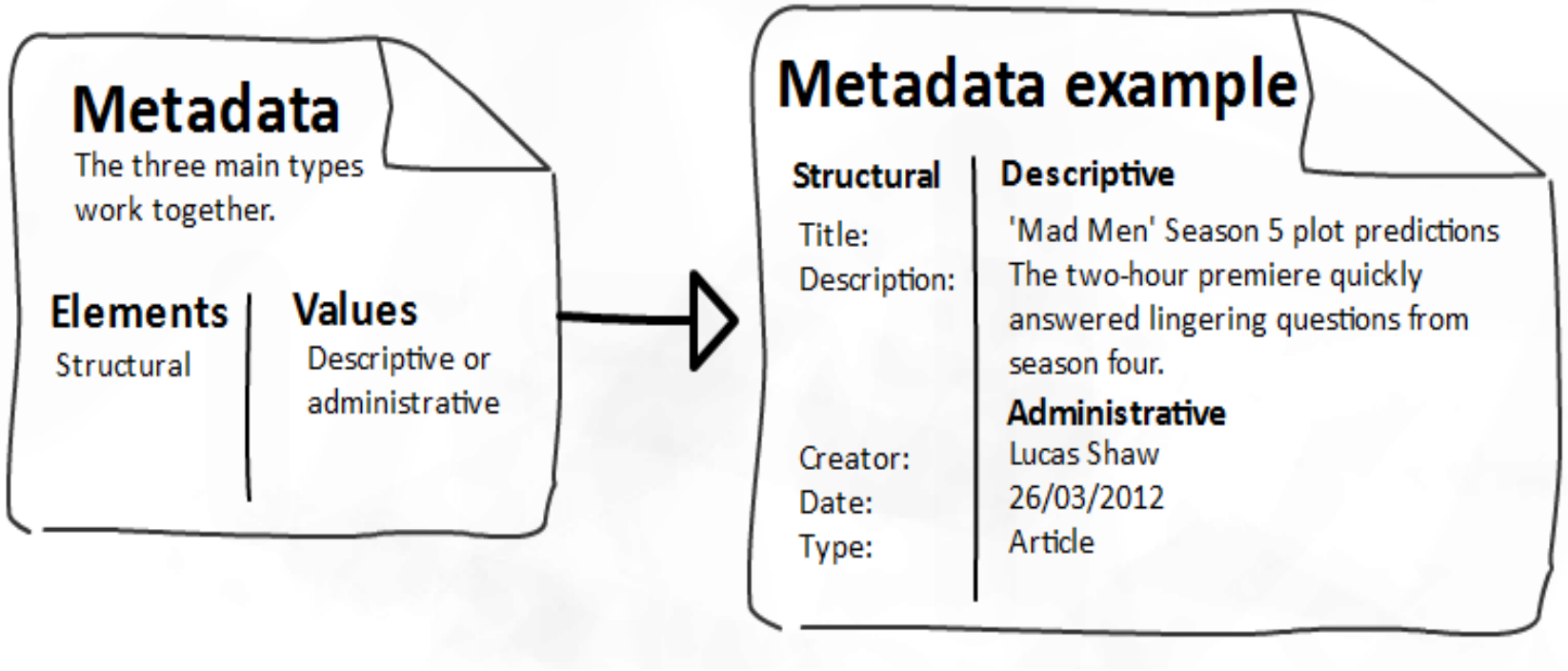


Integrity & Authenticity

Techniques/processes:

- Metadata
- Encryption
- Access control and security
- Check sums/hash algorithms
- Audit trails and access logging

Metadata - provides meaning, access, context and chain of custody verification for electronic records



Categories of Metadata

Descriptive: Describes the intellectual content of a resource for indexing and access.

Administrative: Management information about the digital resource, such as ownership and rights.

Structural: Used to display and navigate digital resources and describe relationships between files.

Technical: Describes the features of the digital file, such as resolution.

Preservation: Facilitates management and access to digital files over time.

Access Control

Identification – who the user claims to be

Authentication – verification that the user is who it is claimed to be

Authorization – what the user has access to and what the user can do with, or to it

- types of records
- ERM system features

Electronic Audit Trails

Capture information such as:

- Record creation information
- Access and usage
- Changes to records and/or metadata
- Changes to classification
- Disposition information
- Changes to system configurations

  etc.

Know When to Say Good-Bye

- Stick to your retention schedule
- Identify **R**edundant, **O**bsolete, **T**ransitory records
- Apply appropriate disposition methods
  - Destruction
  - Accession / transfer
  - Archive (long-term / permanent)
- Monitor, verify and document disposition actions

Inconsistent practices may impact public trust and confidence

The Problem with "Over-Retention"

Storage is cheap, but:

The greater the record volume the higher the:

- Cost of storage system maintenance
- Cost and complexity of migration
- Time to access or search records
- Overall risk to information loss

- **Should records be accessible past their retention period?**
- **Should there be a "right to be forgotten"?**

News Flash!

New Technology Said to Preserve Data for 1,000 Years

(from Information Management magazine, Nov./Dec. 2014)

"Hitachi Data Systems announces a digital preservation platform using Blu-ray technology which allows storage up to 50 years and eventually up to 1,000 years."

Immediate Action Steps

What you can go right away:

- Review storage conditions
- Inspect records and media for degradation
- Review the adequacy of metadata
- Use standard, open file formats
- Adopt standards
- Conduct a *preservation readiness* assessment

Standards Organizations

International Organization for Standardization (ISO)

National Archives and Records Administration (NARA)

Assoc. for Information and Imaging Management (AIIM)

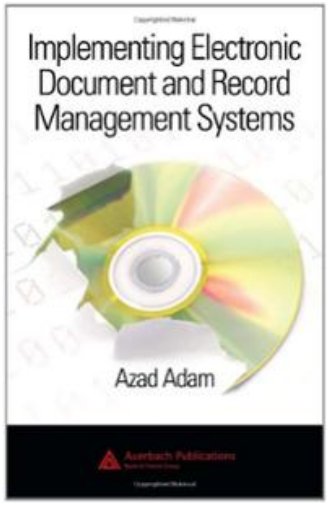
American National Standards Institute (ANSI)

ARMA International (ARMA)

Department of Defense (DoD)

European Commission (MoReq2)

ERM Resources



ARMA International – www.arma.org

Association for Information and Image Management – www.aiim.org

National Archives and Records Administration – www.archives.gov

Council of State Archivists - www.statearchivists.org

National Association of Government Archivists and Records Administrators – www.nagara.org

In Summary…

Know What You Have – take an enterprise view

Know Your Capabilities - evaluate current technical, staff, and financial resources

Know Your Vulnerabilities – assess and remediate risk

Know Your Options – understand and apply appropriate strategies

Know When to Say Good-Bye – stay current with your retention schedule

Join Us at CTC15

Sessions include:

- Electronic records access
- Managing social media
- Digital preservation maturity model
- Emerging policies and practices
- Cloud computing
- E-mail management

...and more


…if all else fails!