

Records Management Audit Trails

Who did what when and who cares?

A presentation for ARMA Houston's 2005 Annual Conference

By Linda J. Mercer

President

Information Network International



Trail Topics

- Accumulation
- Management techniques
- Retention practices
- Compliance expectations



Definition

- Webopedia defines audit trails as:
 - "A record showing who has accessed a computer system and what operations he or she has performed during a given period of time."



Audit Trails

- Document accountability
- Are not retained in some environments



Records Management

- Audit trails are created and retained to satisfy reporting requirements for
 - Item tracking
 - Individual's activities
 - Request
 - Perform
 - Insert
 - Update
 - Delete
 - Compliance and attestation



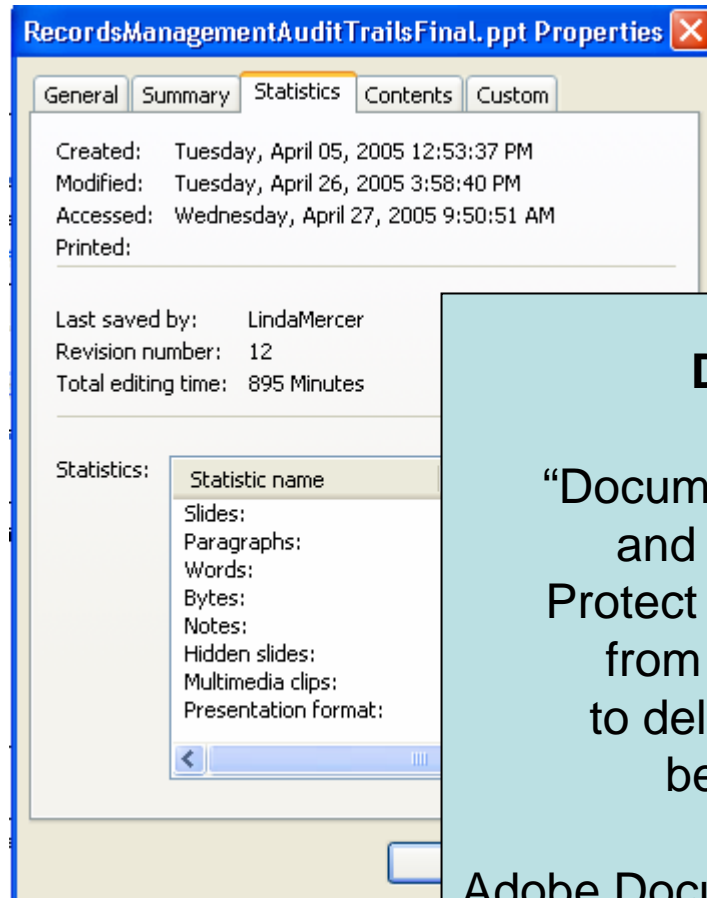
Potential Trail Entries

- Access
- Archive
- Create
- Destroy
- Distribute
- Process
- Receive
- Request
- Retain
- Revise
- Use



Trail Sources

- Devices
- Networks
- Servers
- Applications
- Databases
- Documents



DRM

“Document control and security
Protect documents from creation to delivery and beyond”
by
Adobe Document Services



Data Controls & Gaps

Data management		
Internal Control	Test for Internal Control	Ecora Report for Test
Policies exist for handling, distribution and retention of data and financial reporting output.	Review documented policies and determine if they are adequate and reviewed periodically.	Not Applicable
Retention periods and storage terms for all incoming and outgoing data are clearly defined.	Review written procedures for completeness and adequacy	Not Applicable
A backup and recovery plan has been implemented	Review plan for completeness and relevance.	Not Applicable
	Restore selected configuration data and compare to see if its accurate	Change Report
Confirm no unauthorized changes occur in financial relevant infrastructure	Review selected server configuration data and compare with baseline data	Consolidated Change Report



Trails Accumulate Quickly

1. Verification of activity
2. Queries are not generally maintained though they may be considered useful when monitoring mischievous behavior



Scheduling Trails

- Purpose
- Use
- Access
- Format
- Retention



Scheduling Trails

- Purpose
 - Internal Reporting
 - External Reporting
- Use
 - During life
 - After life
- Format
 - Digital
 - Physical
- Retention
 - Shorter than the item
 - Longer than the item
- Access Security
 - Read
 - Manage



Trail Considerations

- Ownership
- Date and time handling
- Bulk processes
- User identifiers (people)
- Item identifiers (things)



People

- Individual's
 - Activities
 - Assigned Security



Things

- Items
 - Select, Insert, Update, Delete
 - Identification Data
 - Taxonomy
 - Descriptive Terms
 - ‘Serial Numbers’
 - Dates
- Locations
- Standards
 - Templates
 - Data Integrity Rules
- Policy



Trail Workflows

- Reviews
- Storage
- Archives
- Acquisition
- Divestiture



Related Definitions

- Backup
Copy to overcome
disaster
- Archive
File into a
historical
depository



Visual Thesaurus Copyright Thinkmap Inc 2005



Trail Management

Secure Audit Trails

- Minimize who can manipulate them
- Remove trails on a regular basis

Destroy or Archive?

- Purge by type or date of entry
- Preserve in a historical archive



Trail Management

- Monitor information that's critical from a security point of view
- Manage to higher level of protection and audit
- Optimize performance and maximize usefulness of the audit log



Archiving Trails

Create Historical Report

- Capture related data from more than one table
- Retention options
 - physical media
 - digital media
 - database formats
 - text files with labels and comma separated values
 - xml files with labels and data



Who Else Cares?

SOX SEC 404

MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

- (a) each annual report contains an internal control report which
 - (1) states management's **responsibility** for adequate internal control structure and procedures;
 - (2) contains an assessment **of the effectiveness** of the internal control structure and procedures
- (b) each reporting firm shall **attest to and report on** the assessment made by the management of the issuer



Compliance Expectations

03 Sep 2003: FDA final guidance for 21 CFR 11.

2. Audit Trail

- 239 --- 241 ...
- 242 for example, date (e.g., § 58.130(e)), time, or
- 243 sequencing of events, as well as any requirements ensuring that changes to records do not
- 244 obscure previous entries.
- 245
- 246 Even if there are no predicate rule requirements to document, for example, date, time, or
- 247 sequence of events in a particular instance, it may be important to have audit trails or
- 248 other physical, logical, or procedural measures in place to ensure the trustworthiness and
- 249 reliability of the records.
- 250...-252...
- 253 Audit trails can be particularly appropriate when users are expected to
- 254 create, modify, or delete regulated records during normal operation.



Compliance Expectations

- *5. Record Retention*
- 299...308...
- 309 FDA does not intend to object if you decide to archive required records in electronic format to
- 310 non-electronic media such as microfilm, microfiche, and paper, or to a standard electronic file
- 311 format (examples of such formats include, but are not limited to, PDF, XML, or SGML).
- 312 Persons must comply with all predicate rule requirements, and the records themselves and
- 313 any copies of the required records should preserve their content and meaning. As long as
- 314 predicate rule requirements are fully satisfied and the content and meaning of the records are
- 315 preserved and archived, you can delete the electronic version of records. In addition, paper
- 316 and electronic record and signature components can co-exist as long as
- 317 predicate rule requirements are met and the content and meaning of records are preserved.



Investigators

- “Identify as many sources of logs as you can...There is usually a finite life of logs.”

High Technology Criminal Investigation Association

- Legal Issues
- Open Kiosks in public places
 - Liability issues
- Honeypots and entrapment



Compliance Framework

- Assess
- Attest
- Sustain
- Improve

