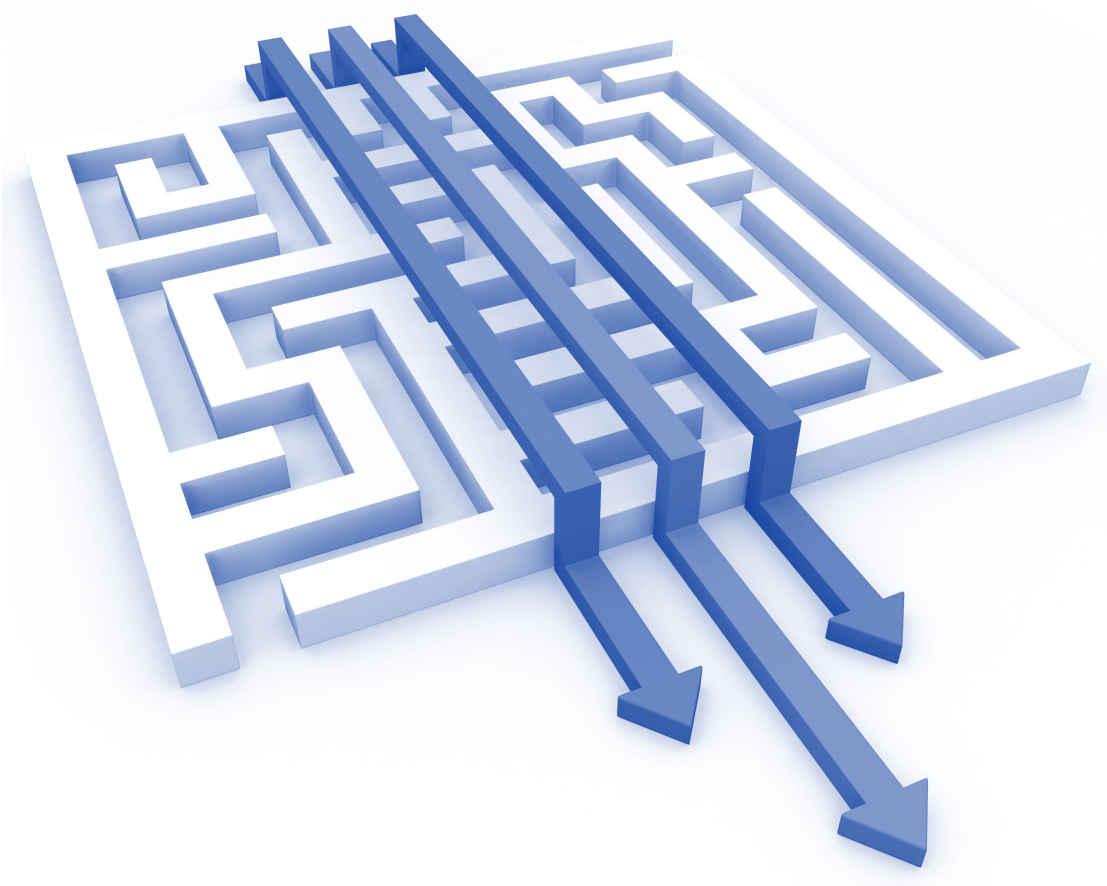


Executive Brief

An Introduction to eDiscovery

From **Archive360**

ARCHIVE360
Point. Click. Migrate.

Introduction

The Archive360 Executive Brief "Introduction to eDiscovery" is intended for organizations that are considering migrating their legacy email archive. The document describes the basics of eDiscovery, introduces the key processes and terminology and highlights the challenges that all companies face during eDiscovery. Most importantly, the document provides a checklist that IT and legal teams can utilize to ensure that any planned migration projects do not alter or compromise their data and impact or jeopardize ongoing or anticipated litigation.

Recommendations

Whenever enterprise data is being moved, migrated or disposed of, care should be taken to ensure that an organization's legal requirements are not being overlooked. Archive360 encourages any organization considering an email archive migration to work with a migration services provider that fully understands your legal responsibilities.

About Archive360

Archive360 is the leader in email archive migration software, successfully migrating more than 10 petabytes of data for more than 450 organizations worldwide since 2012. Archive2Anywhere™, the company's flagship product, is the only solution in the market purpose-built to deliver consistently fast, predictable migration rates, with verifiable data fidelity.

Contact Us

Web: www.archive360.com

Email: info@archive360.com

Phone: +1 (212) 731-2438

+44 (0) 118 328 2069

What is eDiscovery?

Electronic discovery, or eDiscovery as it is more commonly known, is the legal process of identifying, securing, collecting and producing electronically stored information in response to a request for content production in a lawsuit or government investigation.

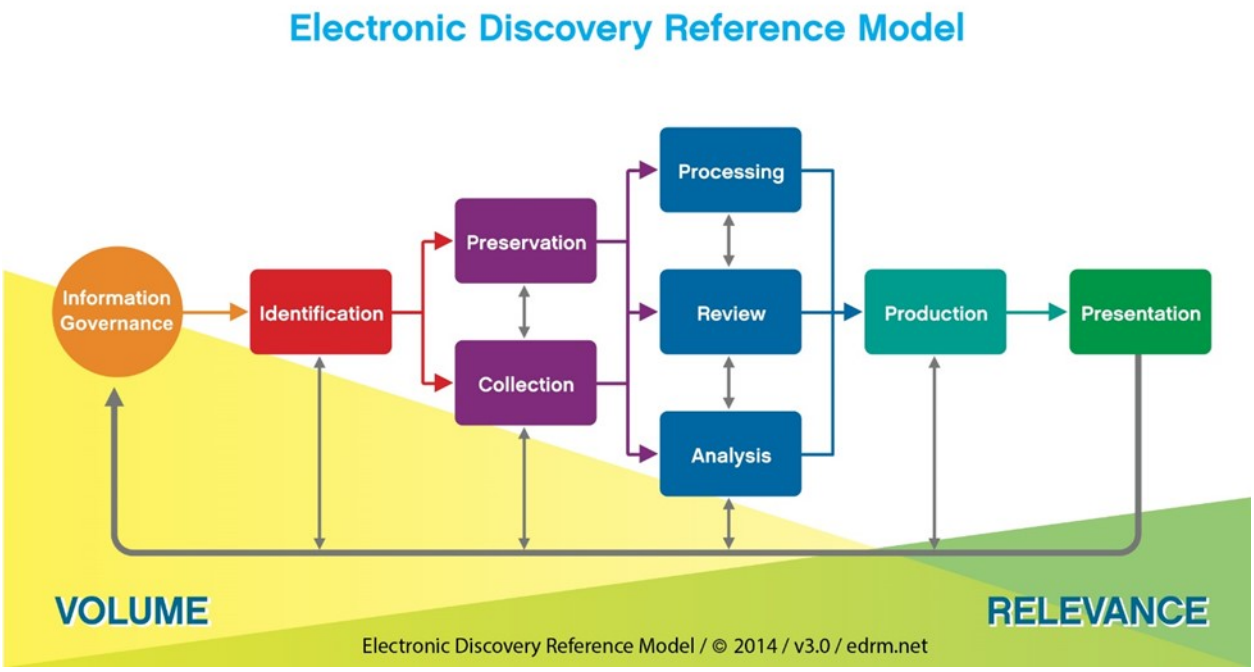
What is Electronically Stored Information (ESI)?

Electronically stored information (often referred to as ESI) can be any electronic file containing content that could be relevant to a given legal matter. ESI can be in any format including but not limited to:

- email
- work files
- databases
- voicemail
- audio and video files
- social media
- web site content

What is EDRM?

The Electronic Discovery Reference Model (EDRM) is an eDiscovery model created by the EDRM industry association in an effort to establish standards and guidelines in the emerging eDiscovery market. The model outlines standards for the recovery and discovery of digital data in response to a discovery request.



Summary Description of the EDRM Stages

Information Governance
Information governance is the management of electronic data in order to mitigate risk and expenses should eDiscovery become an issue - from initial creation of ESI through its final disposition. Information governance is a proactive process intended to reduce overall cost and risk.

Identification
Locating potential sources of ESI and determining the potential data set's scope, breadth and depth.

Preservation
Preservation of data, often referred to as litigation (or legal) hold, ensures that ESI is protected against inappropriate alteration or destruction.

Collection
Gathering all potentially relevant ESI for further use in the eDiscovery process (processing, review, etc.).

Processing
Reducing the volume of ESI and converting it, if necessary, to forms more suitable (and cost effective) for review and analysis.

Review
Evaluating collected ESI for relevance and privilege.

Analysis
Evaluating ESI for content and context, including key patterns, topics, people and discussions.

Production
Delivering ESI to others in appropriate forms and using appropriate delivery mechanisms.

Presentation
Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native and near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

eDiscovery Challenges

The processes and technologies involved in eDiscovery are often complex, time consuming and costly because of the sheer volume of ESI that must be collected, reviewed and produced in a legal case. Additionally, unlike hardcopy evidence, electronic documents are more dynamic and contain metadata such as time-date stamps, author and recipient information, traces of its passage, and file properties. Preserving the original ESI content and associated metadata is the first priority of the eDiscovery process in order to eliminate claims of spoliation (destruction of evidence) or evidence tampering.

The relative cost of producing ESI in response to eDiscovery is:

Collection	8%
Processing	19%
Review	73%

The total cost of reviewing content for relevance averages $18,000 per GB.

RAND Institute for Civil Justice

Know where your data is. It makes a big difference if it's on your network now, or if it's stored somewhere else on backup tapes. Don't walk into a required eDiscovery "meet and confer" session with the opposing counsel without knowing. Again, data topology mapping helps you analyze your ESI and preserve the "right" amount of ESI without under- or over-preserving.

Proactive eDiscovery: The Key to Reducing Litigation Risks and Costs

Data Preparation

Once data criteria is identified by the parties on both sides of a legal matter, all potentially relevant content (both electronic and hard-copy materials) is searched for across all potential data repositories and placed under a litigation hold – a process to protect the content (and metadata) from modification or deletion. After a preliminary culling process to remove obvious duplicates or other non-relevant system files, the remaining data is collected and analyzed to further cull the potentially relevant data set. The remaining content is hosted in a secure environment and made accessible to reviewers who evaluate and code every file for privilege, confidentiality or relevance to the lawsuit. All documents deemed responsive to the suit are then turned over to the opposing counsel.

Discoverable Data

For good cause, the court may order discovery of any content that is not privileged (or confidential) and is relevant to the subject matter involved in the suit – no matter where it resides. In layman's terms, if ESI is *potentially relevant to the case*, you may be ordered to produce it. You should always keep in mind that anything and everything is potentially discoverable.

Federal Rules of Civil Procedure - FRCP

The December 2006 amendments to the Federal Rules of Civil Procedure (FRCP) established a series of expectations about how litigants in federal court will handle ESI in both pre-trial presentation and eDiscovery. The 2006 amendments left little to interpretation - if potentially relevant content is destroyed or lost, the court (and jury) can assume it was lost on purpose. While specific sections of the amendments addressed the problem of the destruction of records as a result of routine or good-faith operations, new amended Rule 37(e) added language that underscored that this was not intended "to provide a shield for the destruction of information related to a litigation."

Archiving and eDiscovery

The amendments to the FRCP and the subsequent enforcement of discovery obligations have emphasized the need for corporations to better control all of their electronic data, including email, in a more systematic way. The result has been the development by organizations of information governance programs and the adoption of archiving technologies. Over the past decade, arguments have been made that ongoing archiving reduces the costs and risks inherent in the discovery process by significantly reducing the time, effort and uncertainties usually required in the identification, preservation and collection stages of the EDRM process.

eDiscovery for litigation demands fast, accurate and defensible responses to electronic data requests. Yet enterprise data is traditionally located in data silos that force an uncertain and awkward eDiscovery process. This poor level of eDiscovery ends in slow, limited and expensive data collection, which itself impacts the time needed for the intensive early analysis and document review processes.

eDiscovery and Unified Archive Repositories

Archive Migration and eDiscovery Concerns

Many organizations have reached the point where they need to migrate their current legacy archiving system to another vendor or solution, due to changing IT strategies, lack of capabilities, rising costs, or End of Life. Unfortunately, the majority of the migration technologies available have not been designed to maintain the fidelity of the archived email message nor to provide a defensible chain of custody in the event of a discovery order.

Before planning a migration, IT teams and records managers should speak with their corporate legal department or outside law firm to discuss and address the following:

1. **Is the organization currently involved in any lawsuits?**
   This question is critical as a sloppy migration process can adversely affect current litigation.
2. **Is any content in the legacy archive currently under a litigation hold?**
   Content secured under a litigation hold is considered by the courts to be legal evidence, and because of that, cannot be altered or destroyed (or lost).
3. **Is the organization anticipating future lawsuits?**
   Just like the above situation where you are already in litigation, anticipation carries the same legal responsibilities – there is no legal difference between anticipated and current litigation.
4. **Is maintaining archived content in its original state, including metadata, a requirement due to current or anticipated litigation?**
   The migration process performed by the majority of archive migration vendors will alter the data, i.e. conversion to another format, loss of metadata, loss of attachments, etc.
5. **Can archived legacy data be migrated to a new platform while maintaining legally defensible chain-of-custody?**
   Chain of custody - the chronological documentation or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence in an unaltered state, can determine if evidence can actually be used during trial. Parties wishing to utilize ESI to back up their case may have to prove the data has not been altered in any way, an almost impossible feat if you are not able to demonstrate and document complete chain of custody.
6. **Did the current legacy archive utilize short-cuts/stubs as a storage management capability?**
   Many archiving systems automatically move email message sand/or attachments from the user's mailbox to the email archive and replace it with a pointer to the archive (known as a "stub" or "shortcut"). This process is designed to be transparent; end-users cannot tell which mailbox items include stubs and which ones are "whole" messages. During a migration project, incorrect migration of stubs causes them to stop working , generating error messages to the end-user and dramatically impacting productivity. Message stubs can also include additional metadata generated from their movement from folder to folder within Exchange. This additional metadata could be relevant in litigation so message stub metadata should not be arbitrarily deleted but instead recombined with the original archived message.
7. **How will corrupt messages be identified and handled?**
   All archiving software creates some level of data corruption. Is the migration software capable of pinpointing the root cause and recovering "soft" corruptions? How will this information be captured and reported?

Whenever enterprise data is moved, migrated, or disposed of, care should be taken to ensure legal requirements are not being overlooked. Ensure you work with a migration services provider that fully understands your legal responsibilities.