## AGENDA

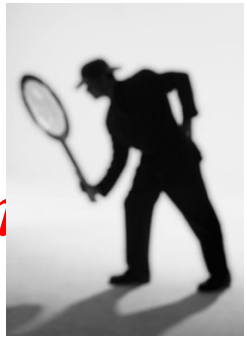

Discovery of electronic evidence

Identification of data


*Information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software.*

## E discovery

- *Gathering , managing, presenting & preserving electron evidence*



## Forensics and E-Discovery

**E-Discovery**

- Gather, filter, evaluate and produce
- Volumes of data from active and archived sources
- Someone else does analysis to build case

## Discovery of Electronic Evidence

*The discoverability of the electronic files is referred to as "Discovery of Electronic Evidence or DEE*

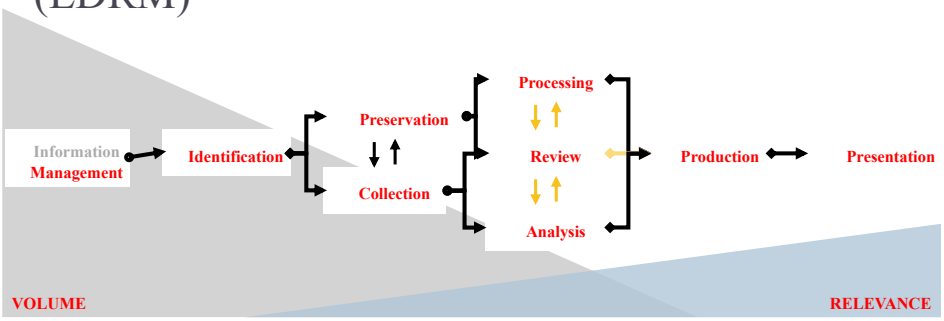
## Types of electronic records typically sought/produced in Discovery


- *Text*
- *Image*
- *Calendars*
- *Databases*
- *Spreadsheets*
- *Animations*
- *Websites*
- *Computer programes*
- *PDAs*
- *Digital signatures…*

## Importance of E- Discovery


- More than 90 % of records created are in electronic format
- More than 70% of electronic info never printed
- Estimated 247 billion mails send every day

## The Electronic Discovery Reference Model (EDRM)




**Information Mgmt:** Define and enforce retention policy

**Identification:** Determine the scope, breadth and depth of ESI

**Preservation:** Ensure ESI is protected against destruction

**Collection:** Gather ESI from various sources

**Processing:** Convert ESI to form suitable for review and analysis

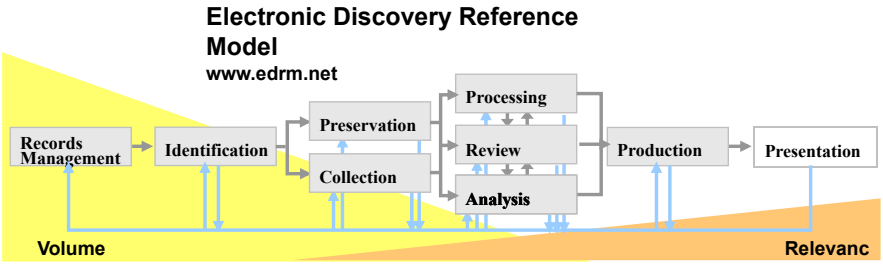
**Analysis:** Evaluate ESI for key topics, people, discussions, etc.

**Review:** Conduct review for privilege and relevance

**Production:** Deliver ESI in appropriate format (e.g., redacted, in TIFF, etc.)

**Presentation:** Display ESI at depositions, hearings, trial, etc.

# What Is EDRM?






- Six-step methodology broken into nine processes
- Developed by a large and diverse group, including vendors, law firms and corporate legal departments
- Common definitions and a working glossary are available in public domain
- Additional work is under way to develop metrics and XML schema

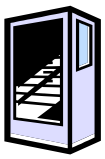
# Preparing for E-Discovery Through Records Management

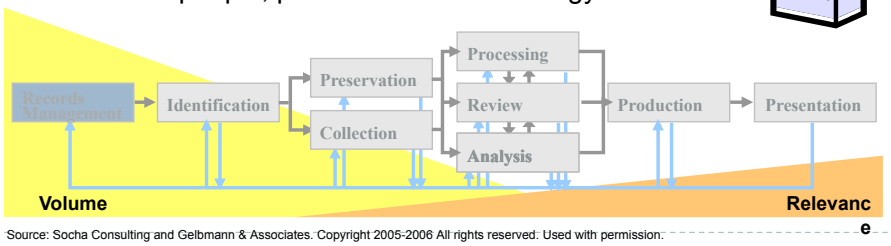
**Who:** Information Management Steering Committee, Corporate and Divisional Records Directors, House Counsel

**What:** Develop a process and solution for declaring, classifying and managing an organization's documents

**When:** Immediately

**How:** As a discipline, records management is completely independent of technology that must address, in this order: people, processes and technology.





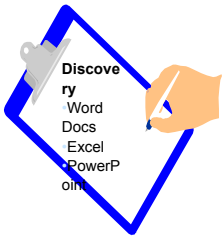
# Proactive Identification of IT Assets

**Who:** Primary responsibility of the IT department

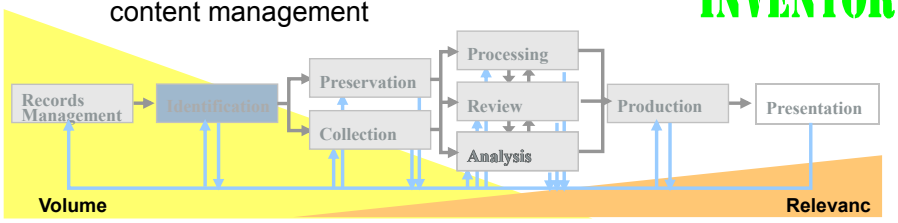
**What:** All hardware, software and storage, backup and recovery, information retention and deletion policies

**When:** Within 90 to 120 days of the cause for action

**How:** IT asset management software, forensics, policy management, records management, content management




INVENTORY





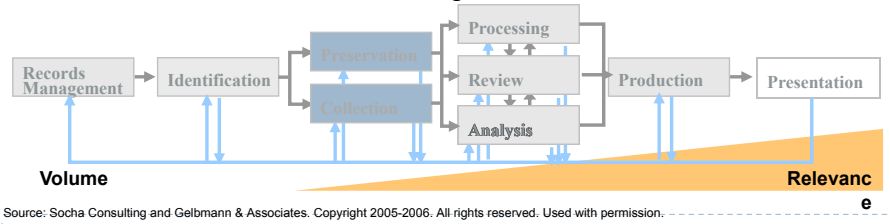

# Preservation and Collection of Evidence

**Who:** IT, acting on the advice of legal counsel or other advisors

**What:** All data and metadata in all systems by custodian, date range and subject matter

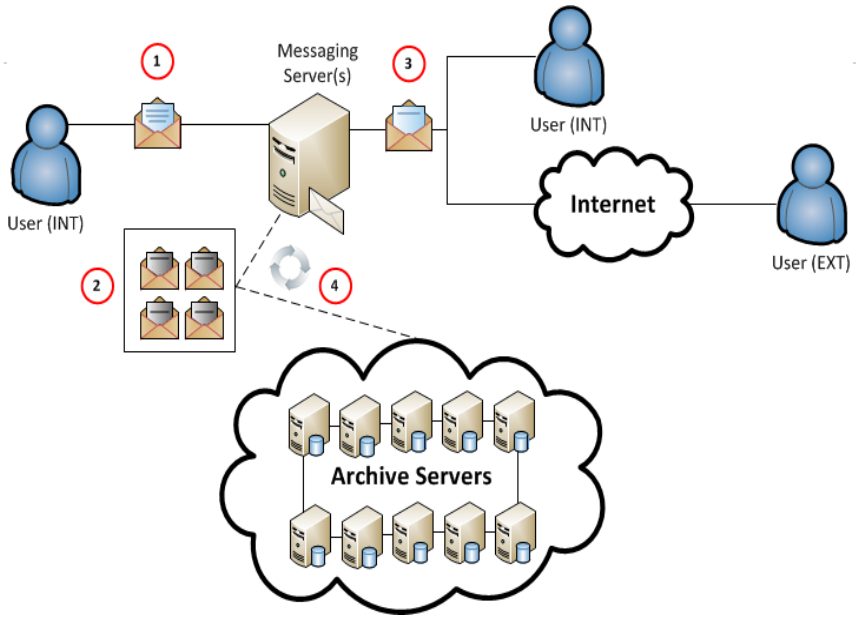
**When:** If you believe information is going to be requested, or immediately upon request


**How:** Content and records management systems, policy management systems, litigation support databases, information access technologies, forensics



## Archiving architecture

- While each organization will tailor its archiving infrastructure according to its specific business requirements, there are typically two common architectures that are used.
- ***Hosted Messaging Archive Solution***
- An organization may choose to rely on a third-party vendor to host their e-communications in a cloud-based environment



- User sends a message to a number of internal and/or external recipients
- A copy of the message is kept in the ‘messaging store’
- The original message is delivered to the intended recipient(s)
- Ingestion occurs at regular intervals to move the messages from the ‘messaging store’ to the archive servers in the cloud.

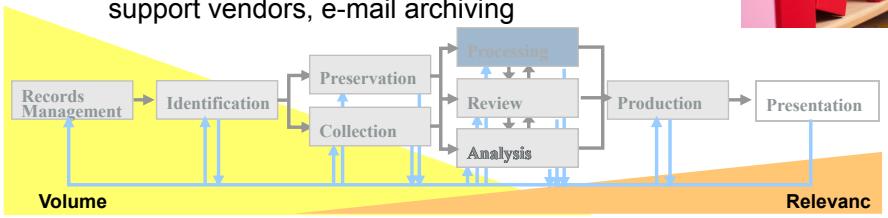
## Processing

**Who:** IT, acting on the advice of legal counsel and using the appropriate tools, third-party provider

**What:** Reduce the overall set of data you have collected by setting aside files that are duplicates, nonrelevant file types

**When:** Upon receipt of interrogatory or subpoena

**How:** Deduplication technology, forensics, litigation support vendors, e-mail archiving



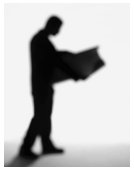
# Review and Analysis: Key Technology Differentiators

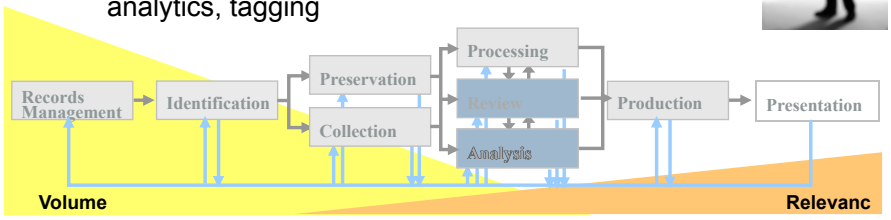
**Who:** Legal professionals, document review software, content analytics

**What:** Review documents for relevancy, privilege and redaction

**When:** Deadlines agreed to in meet and confer conference and set by the court

**How:** Search and information access tools, content analytics, tagging







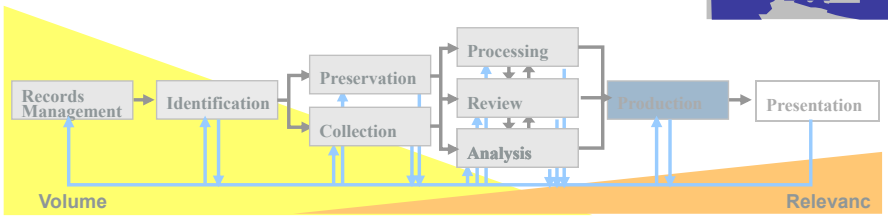

# Production and Presentation

**Who:** Legal professionals, third-party specialists, IT

**What:** The transmittal of relevant material to opposing counsel and the display of evidence during proceedings

**When:** As soon as material is analyzed for production

**How:** Mutually agreed upon format, or in the manner it is used in the normal course of business



## Identification of data

**Time Travel**

None of the clocks in the system are synchronised unless the computer in question is running with NTP ( Network time Protocol)

- NTP is build on top of TCP/IP that ensures accurate time keeping with reference to radio, atomic clock…

Keeping accurate time is very crucial in case of digital evidence

## Identification of data

**Clock Filters**

- NTP guards against changing the system clock
- NTP assumes time moves forward not backward
- Small changes are acceptable
- Making large changes is very time consuming

## Autokey

- Version 4 of NTP has more security improvements.
- A system called the Autokey uses public key algorithms combined with list of one-way hashes
- The client can check the signature send by the server