

What IT Needs to Consider for Legal Hold

What Auditors Should Look For

David Maxwell
David@DavidDMaxwell.com



Legal Hold Considerations for IT

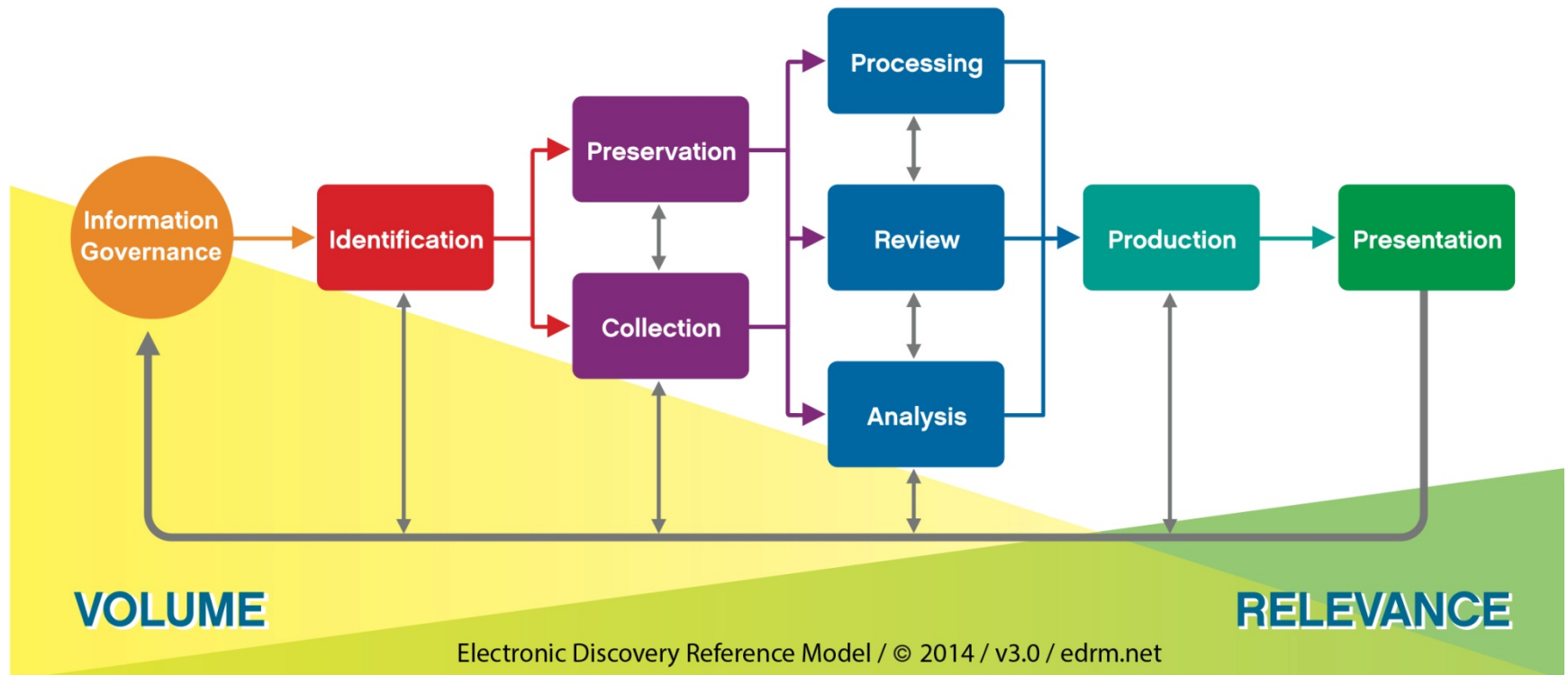
- This presentation is based on my experiences in dealing with IT Legal Holds and Legal Matters.
- This does not reflected any advice from my current employer. These are my opinions.
- Review the considerations with your Legal team for agreement.
- I am not an attorney.

Legal Hold Considerations for IT - Why

- The FRCP in 2006 was updated to include "electronically stored information" Commonly referred to as ESI.
- Legal matters are one of the largest unknown expenses to a business. However, there are few controls to ensure data for legal matters.
- What IT needs to know about Legal:
 - Legal does not know IT
 - Legal often work in silos not always interested with other matters of the legal department
 - IT must work to understand what Legal needs
 - Legal advises they need everything relevant

Legal Hold Considerations for IT – EDRM

Electronic Discovery Reference Model



Legal Hold Considerations for IT - Data

- Two types of data: Structured and Unstructured.
 - Structured: Systems, ERP, CRM, structure systems usually have databases and a defined information structure.
 - Unstructured: User systems (laptops desktop), user file share, dept file share
 - This presentation is related to unstructured data.
- Key considerations of data preserved: Data, Metadata, especially dates-creation, modified, last accessed
- Recommend discussing with Legal to ensure they have an understanding that IT cannot control actions of user on legal hold. If the user decides to purge data, IT cannot ensure that their data is preserved. This applies to data users have control over, such as local computers, file shares and devices. The custodians on hold are expected to apply due diligence to ensure data is preserved.
- My approach: Preserve data associated with custodians as a **whole and do not try to cull or search data**. That is a separate process and should be left to eDiscovery professionals and their tools to analyze and testify how it was found.
- Collection approach: Active data vs Forensic data

Legal Hold Considerations for IT - Notification

- Legal hold notification to CIO, Directors or VPs of IT.
 - Legal usually has one process of legal notification and that is a legal hold. However, many notified should not be put on hold but need awareness.
 - CIO sends email to key staff stating we have a legal hold with these people. Staff really does not know what to do. I recommend identifying a coordinator role, legal IT liaison. A coordinator to ensure custodian lists, procedures and Data is being preserved.
- Recommendation: Establish a CIO owned mail group (better if legal owned) that contains all “need to know” IT people of new legal hold. Have legal send the notification to the mail group. May be best if other departments (such as HR) have this as well.
- The rest of the presentation will provide areas consideration for it to ensure preservation of data.
- Control: IT shall define process for notification of a legal hold to key IT personnel.
- Risk: Preservation may not occur if notification does not happen.

Legal Hold Considerations for IT – Custodian List

- Create a List of custodians (people) on hold.
IT really needs 2 list.
 - List one to use in IT process to identify custodians
 - List two to manage overall custodians and matters
- Do not use any PII data, like SSN#
- List 1: First Name, Last name, employee number
- List 2: First Name, Last name, employee number, date placed on hold, date removed from hold, termination date, matter 1, matter 2
It may be possible that Legal maintain, however with silo structure of most legal groups they may not be centralized.
- Control: IT shall create and maintain a readily available list of active custodians for legal matters. Periodic reviews shall occur with legal to ensure accuracy of the list.
- Risk: IT does identify users that need to have their data preserved for legal holds

Legal Hold Considerations for IT – Custodian List

- List 1

First Name	Last Name	Employee #
David	Maxwell	123456

- List 2

First	Last	EMP #	Date On	Date Off	Term Date	#2014-12	Matter 2	Matter 3
David	Maxwell	123456	1/15/15			3/15/15		

Legal Hold Considerations for IT – Secure Storage Area

- Secured IT storage location for storing assets related to legal matters.
- Need processes if encryption is used on assets.
- Needs a complete Inventory managed of what is stored. I prefer to have this outside of IT control, if possible. Chain of custody (example at ASDFED.com) needs to be applied to each asset. Assets stored may be on more than one legal hold. Over time, this will happen.
- If Legal feels comfortable, you may be able to image to a secured share.

Control: Assets collected for legal hold shall be securely stored, inventoried and managed.

Risk: Collected assets for legal hold are not secured and maintained for collection.

Legal Hold Considerations for IT – Email

- Almost always the #1 area of interest.
Users have a tendency to hoard information and email is the main area they think they need to keep everything. Email is a communication tool. People send emails not just create and store, therefore the receiver should have the email as well.
- Legal Hold server Configuration: Understand if your mail system has ability to apply legal hold. Exchange 2010 and later have this capability. If available, make sure you have documented process in place to insure that custodians have the legal configuration applied. Cloud solution should be reviewed to ensure that preservation capabilities are available. O365 does have this as well.
- Backups: Always asked about by opposing counsel. If you have no other way to preserve email, then backups may be your only solution. If images are used vs backups dumps of users may need to be implemented.
- PST's: Generally stored on the local computer, get those when drive is collected
- MSG: Don't forget user can drag email out of Outlook to other storage areas like their desktop.

Legal Hold Considerations for IT – Email

- Recommendation:
 - #1 Document how email is stored and used in your environment. Have it readily available to share with attorneys. This should be a living document that identifies upgrades and changes to the system as well how users use email and how backups are done and accessed.
 - #2 review backup schedule for reasonable retention time frames.
 - #3 Consider adding retention to user email however for legal hold users retention should be suspended.

Control: IT shall have documented process for preserving email for legal hold custodians

Risk: Email may not be preserved for Legal Hold custodians.

Legal Hold Considerations for IT – User Support

- Help desk needs to be aware of legal hold and have processes that ensure the protection of data. If virus, equipment failure, and other problems occur the help desk must be aware of preservation before solving the issue. Many help desk fixes are solved by reimage however, procedures need to be followed to ensure metadata is managed appropriately and not altered.
- Upgrades area often a different team/group they should also reference the list and have procedures that ensure custodian data is not altered.
- This is when the first list is used. They just need to know names or employee number.
Some ticketing systems are beginning to include fields that stoplight legal custodians.

Control: IT shall have documented process for identifying legal hold custodians and process for handling their data so that data is not changed or altered.

Risk: Collected assets for legal hold are not secured and maintained for collection.

Legal Hold Considerations for IT – Terminations

- Custodians will leave. IT will need to make sure the system of a termed user is collected and preserved.
- This process should be part of the off boarding process.
 - HR should participate /awareness of the process
- Consider the need for the manager to retrieve business related information
 - Define a process for managers to request information within a period of time
 - Process can define a longer period of time to keep the drives for senior management
 - Tech's need processes to ensure data is not altered , may need use write blockers

Control: Termed legal hold custodians shall have their data preserved.

Risk: Legal hold data is not maintained for custodians.

Legal Hold Considerations for IT – Disposal /Reuse of media

- **Hard Drives**
Drives and media must have a process for reuse or disposal. The challenge is that many drives are held for disposal for a period of time. Often waiting for enough drives to dispose or periodic times of the year. In the event a new legal hold may come into play it is best to label and inventory drives waiting to be processed.
- Inventory drives as they are added to the destroy/reuse list and when they are actually destroyed. At both times reference the custodian legal hold list (list 1) to ensure preservation is not needed.
- This becomes very important when tracking down a former employee data. The inventory records of destruction can show when the data was destroyed or reimaged.

Control: Assets defined for destruction shall be inventoried, logged and checked if on legal hold prior to destruction.

Risk: Collected assets for destruction may become on legal hold prior to actual destruction of reuse.

Legal Hold Considerations for IT – Closing thoughts

There are many more challenges:

- Automatic process and scripts should be reviewed and suspended such as auto deletion of share drives until collection of preservation can occur.
- Transfers of employees to different departments/countries.
- Share drives, SharePoint, social media should be considered.
- Confidential nature of litigations, no need for IT to know details
- IT needs to have (regular) training and understanding of Legal Holds. They need to know what are expectations, what to do with data and who to contact if unsure about what to do with data.
- Many times it helps if Legal understands the cost and the burden it takes to preserve. Identifying costs may make it easier for Legal to settle.
- If you have periodic recommendation of purging to be compliant with retention schedules consider including Legal hold verbiage to over ride the iactivity.

Legal Hold Considerations for IT

Questions?