eDiscoveryJournal

Unique Perspective. Independent Insight. Pragmatic Advice.

An eDiscoveryJournal Report:

Managing eDiscovery As a Repeatable Business Process

By:

Barry Murphy & Kevin Esposito

About eDiscoveryJournal

eDiscoveryJournal offers unbiased information, pragmatic advice and a unique perspective on hot eDiscovery news, trends, and best practices. Whether you are hoping to gain insight into the news of the day, research the best technology or service solutions, or find expertise that can help to answer your specific questions, eDiscoveryJournal is the e-zine you will want to visit every day.

About the Authors

Kevin Esposito, MBA JD is a contributing Analyst for eDiscoveryJournal and is the Managing Director at Rivulex, LLC where he drives the analysis and implementation of processes and toolsets that are designed to decrease the cost of complying with legal discovery obligations. Kevin is a founding member of the Electronic Discovery Reference Model (www.edrm.net) where he is currently co-chair of the Model Code of Conduct subcommittee. Kevin was previously co-founder of the Discovery Response Team at Pfizer Inc in New York and helped to lead Pfizer's corporate records retention efforts. As the Director of Electronic Discovery at Pfizer, Kevin was responsible for the day to day operation of the IT side of their discovery process and coordinated all electronic discovery worldwide.

Barry Murphy is the founding Principal of Murphy Insights and a thought leader in all things retention – eDiscovery, records management, and content archiving. Previously, Barry was Director of Product Marketing at Mimosa Systems, a leading content archiving and eDiscovery software. He joined Mimosa after a highly successful stint as Principal Analyst for eDiscovery, records management, and content archiving at Forrester Research.

Disclaimer:

eDiscoveryJournal is not a law firm. All expressed opinions and related content are provided for general educational purposes only and should not be considered to be legal advice, even if the author is a practicing attorney. Neither data shared through eDiscoveryJournal nor the information contained herein should be used as a substitute for competent legal advice from a licensed professional attorney in your state.

eDiscoveryJournal believes reasonable efforts have been made to ensure the accuracy of all eDiscoveryJournal original content. Content may include inaccuracies or typographical errors and such issues may be corrected or updated without notice. All eDiscoveryJournal original content is provided "AS IS". While we endeavor to keep all information up to date and correct, we make no representations or warranties of any kind, express or implied, about its fitness for a particular purpose or the completeness, accuracy, reliability, suitability, or availability with respect to the information, products, services, or related graphics. Any reliance you place on such information is therefore strictly at your own risk.

In no event will eDiscoveryJournal nor any of its contributors be liable for any direct, indirect, punitive, incidental, special, or consequential damages or damages for loss of profits, revenue, data, down time, or use, arising out of or in any way connected with the use of the information contained in this document.

Introduction

Most organizations manage eDiscovery on a matter-by-matter basis, stuck in a reactive nightmare that plays over and over. This approach is both costly and risk-laden. Organizations do not have the time, internal skills or tools required to cull down collected data sets. This results in unnecessarily expensive third-party data processing and legal review. The matter-by-matter approach also leads to inconsistencies in how the same data is treated across matters. Multiple handoffs and increased movement of data from application to application and vendor to vendor raises the chances for spoliation and the potential for negative repercussions such as sanctions.

As eDiscovery gains a higher profile in the mainstream news and on the corporate radar, there is a strong desire on the part of corporate executives to reduce both costs and risk. We at eDiscovery Journal believe that the way to accomplish both goals without sacrificing legal defensibility is to approach eDiscovery as a manageable, repeatable business process. This report will examine the components of the eDiscovery process and the role of various constituents (e.g. Corporate legal, law firm, service provider) within that process. It will also explore how technology and service solutions can support managing eDiscovery and the trends that affect decision making, such as the emergence of more integrated eDiscovery platforms.

Contents

![eDiscovery Journal logo]

eDiscoveryJournal
Unique Perspective. Independent Insight. Pragmatic Advice.

Traditional, Reactive eDiscovery Is No Longer Acceptable

In the mid-to-late 1990s, an explosion of digital information began to create a hidden challenge: finding, preserving, and producing electronic information in response to a discovery request, whether for litigation, regulatory action or an internal investigation. As the volume of electronic information grew, so too did the problems associated with eDiscovery. Because the process was immature, eDiscovery became:

- **Reactive and siloed.** Every matter became a fire-fight treated independently of other matters. This led to duplication of effort and the potential for treating information inconsistently across matters. Each discovery request left legal having to wait for data and IT scrambling to collect and preserve information. Legal was unable to adequately articulate what information they needed to prepare for meet-and-confer sessions with opposing counsel. And IT resources were pulled from value-add projects into feverish collection efforts that were likely duplicative.

- **Risk-laden**. Because matters were treated in such a siloed manner, there was a huge risk of treating information inconsistently across matters. For example, many commentators have highlighted the potential for a company to accidentally waive privilege by marking a document privileged in one matter, but not in another. In addition, collection and preservation tended to be siloed by content source (e.g email, desktop, file system). In order to work with such siloed data sources, there developed a need to move data between applications frequently. This increased the risk of spoliation and made managing the chain of custody/possession much more challenging and complex.

- **High cost**. The lack of sophistication in corporate approaches to legal hold created constant over-preservation, which only exacerbated the high downstream costs. Because IT had to collect and preserve information quickly and typically did not have the requisite software tools in-house that would be needed to properly sort and index large volumes of loose files, organizations had no way to efficiently cull down the volume of potentially responsive data. For each matter, a company would be forced to send large collections to third-party vendors for EDD processing at prices that historically were over $2,000 per

GB at times. The lack of a consolidated approach to the processing of these data populations also meant that non-responsive information could not be filtered out of the collection and would wind up being included in the piles of data that were reviewed by high-priced lawyers. Consequently, the downstream costs of eDiscovery rose quickly. Without a defined eDiscovery process, companies were not in a position to define requirements for technical solutions that could help lower costs and reduce risks.

In December 2006, amendments to the Federal Rules of Civil Procedure (FRCP) affirmatively stated the obligations of all parties within the legal system to address eDiscovery as a key to managing litigation. These rules essentially put the burden of conducting full and reasonable discovery squarely on the shoulders of the defendants, who controlled most of the information at issue in larger litigation matters. As eDiscovery hit the mainstream, the spotlight was focused on the high costs and risks related to complying with the new Federal Rules. This forced many companies to address eDiscovery head-on. With a dearth of best practices and an immature market, taking control of eDiscovery has not been easy to date.

Now that the FRCP amendments have been in effect for five years, high-profile court cases with large sanctions have established the potential adverse effects of ignoring eDiscovery. In addition, stories about "eDiscovery gone bad" have been spotlighted in mainstream media such as The Wall Street Journal and The New York Times. This coverage has moved eDiscovery to the forefront of corporate attention. Given the need to manage risk, control costs, and meet the requirements of the FRCP, companies may no longer fail to address the challenges related to eDiscovery. The best way to approach those challenges is to treat eDiscovery as a standard business process – a marriage of people, defined tasks, and technology.

eDiscovery Is Like Any Other Business Process

Due to the artisanal culture within the legal profession, eDiscovery has been viewed as a specialty area, with so many legal intricacies that it could never be standardized or managed as a linear process. To the contrary, eDiscovery is very much like other business processes – it is a series of linked activities conducted by people, informed by data and metrics, and sometimes more efficiently managed with technology.

Electronic Discovery Reference Model

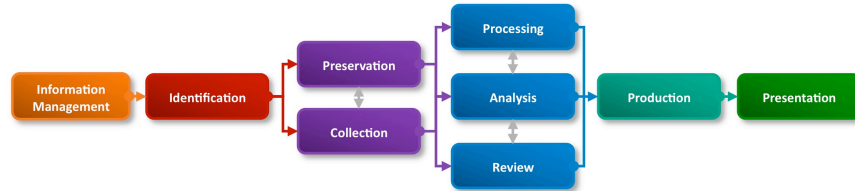Electronic Discovery Reference Model / © 2009 / v2.0 / edrm.net
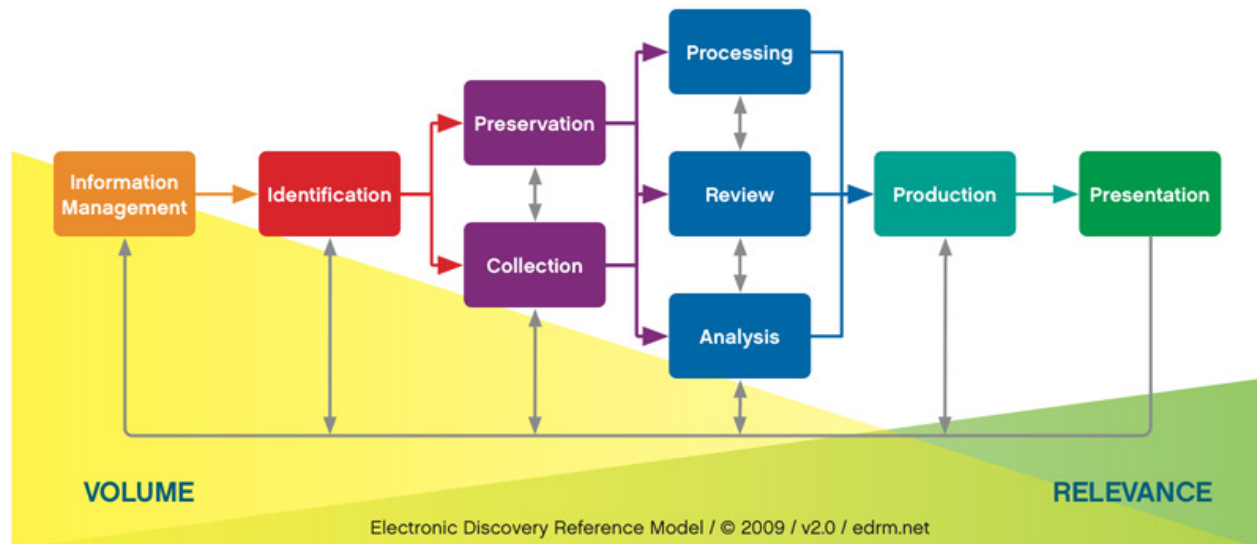
The challenge is that the process itself is more than just the sum of the components. There are literally hundreds of steps that can occur within the eDiscovery lifecycle, and they do not always occur in a linear fashion. Often, a company will find itself bouncing back and forth between various process steps depending on how the matter plays out. Therefore, it is critical for each organization to determine which tasks they can reasonably decide to attack internally and if the resources and wherewithal exist to actually conduct those tasks effectively.

Defining The "eDiscovery Process"

Each organization needs to decide for itself what components of the eDiscovery process it wants to execute on its own. When an organization defines its particular version of the eDiscovery process, it is important to remember that there are multiple constituents that play different roles within that process. Corporations, law firms, and service providers all bring important expertise to the table, but also all must make process and technology, solution decisions that reflect their resources, capabilities, and priority needs. The following graphic depicts some of the more granular tasks within the eDiscovery process:

Breaking Down The eDiscovery Process

Information Management → Identification → Preservation / Collection → Processing / Analysis / Review → Production → Presentation

INFORMATION MANAGEMENT
- Info creation
- Info access (employee)
- Archives
- Info usage policies
- Retention policy creation
- Retention execution (proactive)
- Storage reclamation
- Records declaration

IDENTIFICATION
- Data mapping
  − Custodians
  − Sources
    • Non-custodial
    • Active
    • Legacy

COLLECTION
- Forensic disk imaging
- Search
  − Sources
    • Active
    • Legacy

PRESERVATION
- Legal hold management
  − Custodians
  − Notification
  − Interviews
  − Sources
    • Active
    • Legacy
- Data lock-down
  • In-place
  • Copy & move

PROCESSING
- Create common searchable format
  − Index
  − OCR
  − Convert
- Metadata extraction
- De-NIST
- Culling

ANALYSIS
- Concept search / clustering
- Email thread analysis
- Predictive tagging
  − Machine learning
  − Sampling
- Near deduplication

REVIEW
- Linear document review
- Workflow
- Tagging
  − Privilege
  − Responsiveness
- Redaction

PRODUCTION
- Bates numbering
- Export
- Conversion

Regardless of the eDiscovery task considered or point within the eDiscovery process lifecycle, there are some foundational elements that all organizations must take into consideration. The first is scope. Remember that the FRCP call for companies to undertake "reasonable" eDiscovery efforts. What is "reasonable for any organization will directly impact the scope of how much data is collected and processed. While every organization needs to determine what is reasonable for their specific situation, some considerations for scope include:

- **Custodians**. In many large organizations, there are certain custodians that are likely to be named in many cases. It can make sense to target the first eDiscovery efforts around those custodians' data rather than taking an enterprise-wide approach to begin..

- **Data sources**. Some organizations like to attack the most problematic data sources. Historically, this has meant email archiving: email is often the target of discovery requests because so much of an organization's information passed through email. A

central archive allowed companies to put an end to personal archives (PSTs) that had to be harvested for each eDiscovery effort.

Regardless of where an organization starts, it is critical to understand what data sources exist, the potential methods for conducting collection of those sources, potential hardware and software solutions that may assist with that collection and preservation and firmly establish whether the organization has the ability to deploy and manage those solutions. When considering both collection and processing the client needs to consider the question from both sides of the legal aisle. While the defendant may choose not to employ some of the more complex hardware and software solutions for collection and processing, they need to be aware that the very existence of those solutions could be used against them by Plaintiff's Counsel who may attempt to push for a wider scope on collection, preservation and production.

- **"Forensic" images versus "standard collection**." The largest amount of legal risk resides in the earliest part of the process described by the EDRM diagram. Errors early in identification, collection and preservation can have disastrous results later in the litigation process. When considering collection, for example, there are times when a custodian's full disk image will be required in order to be considered a reasonable effort. This is usually when there is some allegation of data being intentionally hidden or destroyed by the custodian in question. For those instances, a "forensic image" is the only acceptable method for collection and preservation. This usually arises in the context of a criminal matter or a corporate investigation. When there is no such criminal context and/or when there is no allegation of intentional data destruction, there is no requirement for forensic tools to be employed. Organizations are well within the bounds of best practice if they employ less stringent tools for collection and preservation as long as those tools are "forensically sound". By "forensically sound", we mean that there is no chance for data to be unintentionally lost or altered during the collection process. Organizations, therefore, should be sure to have the capability to execute an approach to eDiscovery that utilizes traditional forensic tools when necessary for specific types of matters and technically sound tools for less demanding cases.

Another foundational issue in the eDiscovery process is the management of the chain of custody, or chain of possession. Again, in criminal cases, the term "chain of custody" is the term of art, whereas "chain of custody" has gained favor in all other matters. In order for the court to recognize and admit a document or file into evidence, the producing party must be able to tell the court where the item came from, who collected it, how it was collected and where it has been at every step from its original creator, through processing and right up to production to the opposition or to the court. The corporate user who had 'care, custody and control' of the item is usually referred to as a custodian. Having clear documentation of where, when and how that item was collected along with the inventory of metadata should provide confidence that no loss of data has occurred and no unintentional alteration of the data has taken place.

One of the challenges of managing the chain of custody in eDiscovery is that data moves frequently within the process, either from application to application or from entity to entity, (e.g. corporation to law firm). It is critical to have reports and an audit trail to track all data handoffs to track the movement of data through the eDiscovery process.

Marrying The Reactive With The Proactive

eDiscovery, by its nature, will always be inherently reactive. However, proactive information management can help make the process more efficient. Many companies keep information such as email and file system content in corporate archives. These archives act as centralized repositories and eDiscovery systems of record. Such information may be archived and ultimately removed from production systems in order to optimize production system performance and reduce storage costs by moving the data to a less expensive tier of storage media. Companies can quickly place legal holds on the content in these archives and then extract relevant content to a matter repository when necessary. There will always be a need for tools to collect from other corporate sources of information, especially as new types of information, such as social media, arise. Archives or other content management systems can set the stage for optimized eDiscovery. Marrying a solid information management foundation with eDiscovery tools for collection and preservation of other content can take eDiscovery from a reactive fire-fight to a simple business process kicked off by a request for information or the need to execute a legal hold.

What Leading Organizations Are Doing Today

Very few organizations have a large enough litigation portfolio or a robust enough IT infrastructure to justify taking all of the components of the eDiscovery process "in-house." Leading organizations in this space begin with effectively managing the legal hold process. Many decide to combine the elements of identification, collection, and preservation with some initial level of processing, review, and analysis. This combination of elements is often referred to as early case assessment (ECA).

When implementing legal hold initiatives, organizations tend to focus on the notification process – sending messages of some description to relevant custodians informing them of the existence of the matter and the requirements of the legal hold. Current case law is specific about the need for prompt notification, but effective organizations know that the legal hold cycle does not end with sending the notification. A good legal hold solution will connect the notification and tracking process with the affiliated tasks required to actually preserve content. When preserving data, organizations may find that they cannot simply rely on individual custodians to preserve their data. In some cases, there may be a compelling argument for creating a dedicated area where the content may be preserved. Typically, this is done by copying the data from its original location into a matter-specific preservation repository. However, eDiscovery is not always a linear process that follows the steps in the EDRM in a specific order. For example, some elements of analysis might occur before collection, preservation, and processing. For some matters, it can be helpful to run some level of analysis on data before collecting and preserving it. Scanning potentially responsive data sources for file inventories can help companies understand the volume of potentially responsive data. With that information, a company can make decisions on the potential economics of the case before actually copying the data to a preservation repository.

Once the relevant data has been marshaled, decisions have to be made regarding how to utilize it to support "a claim or defense" within any matter. The logical extension is to develop some in-house capabilities for preliminary processing, analysis, and review. These ECA capabilities can offer some very real benefits:

- **Establishing potential outcomes**. By getting a quick read on the amount of potentially responsive data or even a sense for the merit of the matter, organizations can avoid or minimize downstream eDiscovery costs. For example, a company may use ECA functionality to find the most pertinent information quickly that facilitates a request for dismissal.

- **Avoiding unnecessary costs.** The ability to better cull data down to the minimal universe of potentially responsive information allows organizations to avoid downstream processing and review costs.

- **Achieving performance enhancements**. Earlier insight into matters allows in-house and external counsel to negotiate more effectively at 26f conferences with targeted collection plans, better cost-shifting arguments and defensible undue burden claims.

- **Optimizing collaboration within the eDiscovery process**. Throughout the process, Legal and IT teams must work together to fulfill corporate obligations. Too often, the communication between these teams is weak, resulting in further confusion. A solid eDiscovery technology foundation with workflow built in to enable the process can help in many ways. Aside from cost reduction and better risk management, organizations can achieve better collaboration amongst resources in the process. For example, legal can access the foundation to set up legal holds while IT can access it to execute the collections requested by legal. That helps to clear up one of the big problems in eDiscovery today – finger-pointing between departments because the process is not managed with workflow. The workflow can actually compel strategic collaboration between Legal, IT, Compliance, and Records Management groups.

By taking control of the eDiscovery process and implementing aspects of ECA functionality, organizations can achieve real benefits. Managing business processes like eDiscovery, however, goes beyond the application of technology features; it is critical to ensure that the right people are handling the right tasks. People are an important – often the most important – piece of the puzzle. And, the people involved in the eDiscovery process do not necessarily reside only within the corporation – those at law firms and external service providers play an important role, as

well. Therefore, it is imperative to ensure that the right roles and responsibilities are assigned and tracked; we call this "managing the triangle."

"Managing The Triangle"

Law firms and service providers both play important roles in the eDiscovery process as partners to corporations. Since few corporations can ever justify taking on the full burden of eDiscovery as an internal process they will always use law firms and service providers to augment their internal effort. As a result, there is a need to make sure that all partners have fast access to information, are able to work together simply and efficiently, and that the overall process is defensible and as low risk as possible. The graphic below depicts the "triangle" of the corporation, the law firm, and service providers:

Managing The Client, Firm, Provider Triangle

Corporation

- Effective collaboration
  - Efficient decision-making
  - Project management
- Manage ethical issues
- Transfer of data
  - Minimize movement
  - Chain of possession/custody management

Law Firm

Service Provider

As with all business processes, there is not one right way to set up the triangle and the triangle is not necessarily equilateral. Some corporations will have the power to dictate how their discovery

processes operate and the role played by their outside law firms while others will be forced to have a much greater reliance on the law firms for advice on how to conduct eDiscovery. There is also the issue of conflicting business models. The corporation has a need to minimize the cost associated with discovery and that may put them in conflict with their outside law firms who have historically added to their revenue chain by providing some or all of the processes that corporation now wish to take in-house.

The role of third party service providers is important as well. Even when corporations decide to set up EDD processing capabilities in-house, it is typically for "first pass" processing to cull down the set of information. Rarely do they wish to take the data further than the ECA stage. In part this is due to the volume of work that would take their internal IT staff away from mission critical duties and in part this is due to the realization that the more work that is done internally, the more closely scrutinized their internal processes become. Cost avoidance claimed for doing work in-house may prove illusory if even greater sums are spent on hours expended by lawyers trying to justify and/or defend that work. It is better to allow the service providers to handle more specialized tasks. For example, experienced project managers at service providers can do the data profiling on the initial custodial known-relevant collections and then apply search optimization to support 26f meet and confer scope negotiations. It does not make much sense for corporations to employ this type of expertise internally because the project managers at service providers gain economies of scale by bringing expertise across multiple clients.

Applying Technology And Tools to the Business Process of eDiscovery

In the past decade, a flood of focused point solutions hit the market to help with various aspects of eDiscovery. While providing some good near-term value, for some clients these point solutions also added to the complexity of managing eDiscovery. Corporate IT departments typically do not like deploying multiple tools to solve one problem, but until recently there were few single source applications that could handle all of the facets of discovery. Some of the IT groups advocated waiting for the market to mature before purchasing a solution, while both Legal and Finance people argued that the growing costs demanded some level of a solution be found, no matter how patchwork a solution might result from such efforts. In many cases, ECA appliances were sold directly to legal departments without IT's knowledge or input which helped

to increase friction between those two groups. While all parties agreed that something needed to be done, agreement between them was rarely reached.

For early eDiscovery teams focusing on decreasing risk as well as cost, it became clear that the movement of data from application to application throughout the eDiscovery lifecycle made managing a defensible chain of custody more challenging. The only way to decrease potential risks was to decrease the potential handoffs and the potential points of failure in the overall process. As such, more and more organizations sought to build an eDiscovery foundation with as few tools as possible.
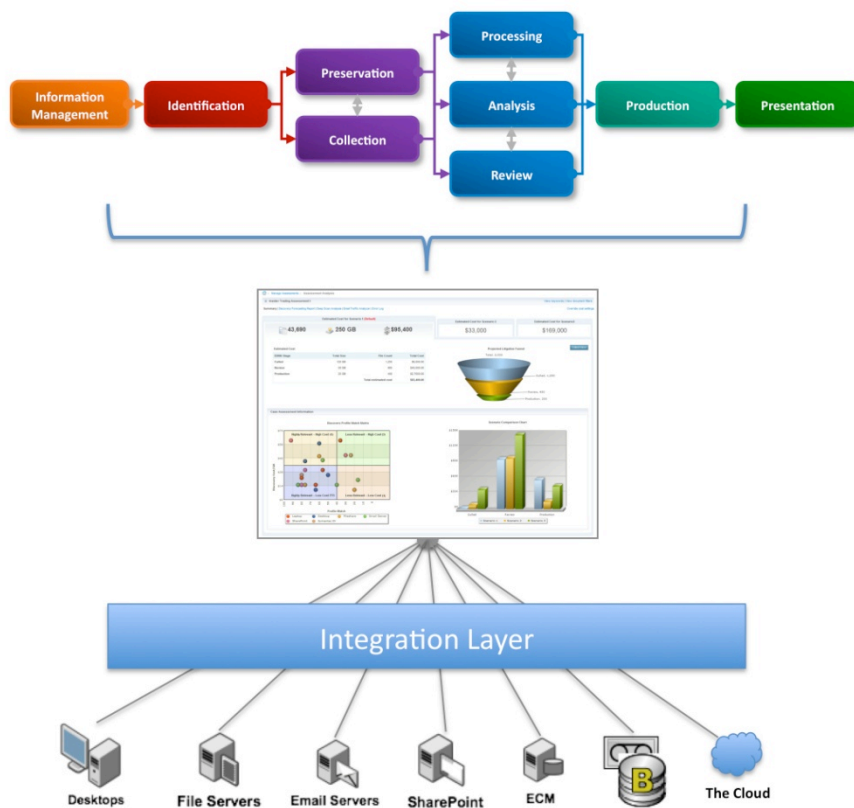
The key to an effective eDiscovery foundation is the central interface to data from various sources. We like to call this the "integration paradigm." As a practical matter, data is never going to be stored in one uber-repository. What companies need is a way to integrate all potentially responsive information with a single gateway or interface that provides access to that

information, such as a unified or federated index structure. Through this interface, various service partners (IT or legal, internal or external) should be able to conduct all necessary and defined eDiscovery process tasks such as:

- Legal hold notification and tracking

- In-place analysis of file inventories with amount of data and breakdown of file types before conducting collection.

- Collection or Collection Management

- Indexing

- Culling

- Search and analytics

- Review

When developing the integration layer, thought should be given to including workflow elements to better track the movement of data through the process as well as the expenditure of resources (whether people or finances). More timely tracking of tasks and expenditures will help to facilitate communication between the process partners and minimize the types of communication errors that multi-party processes are prone to.

Some companies have decided that it may be prudent to leverage business intelligence assets that they currently employ in their main lines of business. BI analysts can help to delve into the specifics of the eDiscovery business process via the central interface to help provide decision-makers within all partner groups with data that facilitates quick decision-making and redeployment of assets. Some groups do this via extensive report writing, while others prefer so called "dashboards" that help to provide high level "status at a glance" information for key decision makers. Some of the metrics that such groups tend to track include:

Historical Metrics (averages)	Matter-Specific Metrics (actuals or projections)
Size: Average GB per matter type	Size: GB/custodian or data source
Costs: $ per GB for processing file types; cost per hour for document review	Volume of documents by data source and file type
Latency: time per GB to collect and review	Special collection or production considerations
Culling rate averages per data source	Dupes and near-dupes counts

Many clients report that the hardest part of working metrics into the process is actually getting the historical metrics. Too often, there is no tracking mechanism to build historical averages or to track how much time tasks like document review takes. Once the tracking begins, however, clients very quickly begin to understand how to leverage metrics for scenario-building. It becomes possible to more accurately predict the way certain cases (e.g. product liability) will play out from a cost perspective. Having a dashboard view of the process with metrics built in allows for better budget planning and faster insight into potential matter costs or red flags.

eDiscovery Is A Team Effort

The eDiscovery business process contains many tasks that are executed by people. In order to effectively manage the process, all the players involved must know their role and understand their responsibilities. While this sounds like common sense, this is actually the area in which most organizations are likely to fail. Because of cultural issues, there is often a tendency to allow roles and responsibilities to "wander" or disintegrate when data volumes and/or time constraints begin to be brought to bear on any particular matter. Over stepping is routine – with lawyers being among the worst culprits. They routinely violate good IT practices and advocate shortcuts if the number of documents in the review room starts to drop. IT people cannot overcome their natural tendencies to be helpful and creative and begin to take on new roles or larger responsibilities regardless of whether those changes are truly in the best interest of the matter at hand. Much of this culture clash is a result not of establishing and allocating roles and

responsibilities early on, but in failing to ensure that those roles and responsibilities are adhered to throughout the process.. Every company will be different, but the following graphic depicts some of the broader roles and responsibilities for the teams involved in eDiscovery:

Get Roles & Responsibilities Right

Legal

- Approve retention and disposition policies
- Execute eDiscovery strategy, e.g. relationship with law firm(s)
- Conduct pre-review of discovered data
- Manage the cost of legal review
- Identify custodians for legal hold

IT

- Choose technology to execute retention, collection, preservation, and review of electronic information (whether for litigation or other investigation needs, e.g. compliance)
- Create budget for technology to support legal, compliance, and business units
- Manage security of the IT and information environment

Business

- Define and communicate information needs and consumption points.
- Communicate lifecycle value of information, e.g. how long knowledge assets maintain value
- Classify information assets

In general, it is best to recognize that legal is the eDiscovery process owner and is responsible for defining the basic requirements for what the organization needs to do internally. IT should ultimately make technology purchases based on the requirements set by legal. As such, both departments need to work together to make a business case for investments in solutions when necessary.

Effective organizations create eDiscovery task forces with representation from many business units, including Legal, IT, compliance, records & information management, as well as several qualified employees to voice the needs of end-users.

Conclusion

In order to relieve the chaos that eDiscovery currently causes for some companies, the key is to treat it like any other business process by defining the elements included in the process, who does what throughout that process and then employing technology where reasonable and cost effective in order to move the process along efficiently. While this sounds simple, it is actually very challenging in practice. eDiscovery is a complex process with multiple components and an evolving solutions market. Some guiding principles to keep in mind when addressing eDiscovery are:

- **Define *your* eDiscovery process**. Every company is different with regard to what process components they are capable of owning, desire to own, and have the resources to conduct. It is critical for companies to actually state what pieces of the process they will conduct internally and then look at solutions. Importantly, owning the process does not mean in-sourcing all process activities. There are external resources such as law firms and EDD service providers that can play an important role in helping a company take charge in eDiscovery.

- **Get alignment of the team players**. As mentioned, eDiscovery efforts will fall apart quickly if roles and responsibilities are not well defined early on. In order to get past the finger pointing and inter-departmental quarreling, everyone involved in the process must be marching to the beat of the same drummer.

- **Think centralization**. While no organization will ever store all information in one uber-repository, it is necessary to be able to collect and preserve any potentially responsive information. In order to make that process efficient, a central interface from which to kick off those preservation notices and collection initiatives is crucial. Effective organizations create an eDiscovery foundation with an integration framework that allows them to touch all discoverable systems. While there will always be a need for best-of-breed tools, it is smart to build this foundation with as few applications as possible. Managing one solution vendor is much more simple than deploying five to ten point solutions.

- **Inform the process**. The beauty of process management is that it enables continuous improvement. As organizations control and measure the process, they will build up

statistics that will allow them to optimize performance. On the theme of a centralized interface, companies can put key metrics into a dashboard within the eDiscovery foundation and make better, faster decisions.

- **Apply Business Process Management (BPM) principles.** Companies employ BPM software to manage all kinds of business process from sales and proposal management to insurance claims processing. When addressing eDiscovery, the same process context applies – it is a marriage of people, tasks, technology, and data.

- **Focus on what is reasonable.** eDiscovery is a complex process involving numerous data sources, multiple stakeholders, and a confusing array of software and service solutions. Addressing all enterprise data right away will be overwhelming. Every company must decide what is reasonable for it to undertake and then map a strategic plan to grow the program. Many start by tackling email and then moving on to other common systems like file shares, desktops, and SharePoint. The important thing is to document data sources, their accessibility, the type of data that exists, and the costs to collect from those sources in order to make defensible arguments for what is reasonable.