

The background features a series of squares of varying sizes and orientations, some solid and some outlined. A series of dotted lines runs diagonally across the page. A small blue horizontal bar is positioned above the title.

THE E-DISCOVERY CHECKLIST MANIFESTO



ACEDS

DigitalWarRoom

AUTHORS:

Tom O'Connor, Gulf Coast Legal
Technology Center

Jeremy Greer, Digital WarRoom

Michael Quartararo, ACEDS

CONTENTS

| | |
|--|-----------|
| INTRODUCTION | 1 |
| The E-Discovery Checklist Manifesto Diagram..... | 1 |
| CONSULTATION | 2 |
| Federal Rules: The Federal Rules of Civil Procedure (FRCP)..... | 2 |
| Client Meeting Checklist..... | 3 |
| Review of Factual Issues | 3 |
| Information Governance Considerations..... | 3 |
| Strategy: Manage Expectations..... | 3 |
| IDENTIFICATION | 4 |
| Data Map..... | 4 |
| Sources of ESI..... | 4 |
| Non-Custodial Sources..... | 4 |
| Custodians..... | 5 |
| Strategy: Plan for Reasonableness | 5 |
| PRESERVATION..... | 6 |
| A Preservation Checklist | 6 |
| Implement a Litigation Hold..... | 6 |
| Strategy: Thoughtful and Reasoned Approach | 7 |
| COLLECTION | 8 |
| Forms of Collection..... | 8 |
| Collection Checklist..... | 8 |
| Strategy: Base Collection on the Needs of the Case | 8 |
| PROCESSING | 9 |
| What Happens During Processing? | 9 |
| A Processing Checklist..... | 9 |
| Strategy: Reduce the Data Set..... | 9 |
| DOCUMENT REVIEW | 10 |
| Reviewing Techniques Are Used to Identify | 10 |
| Some steps to consider to maximize efficiency and organize the document review | 10 |
| Strategy: Consistency | 11 |
| ANALYSIS CHECKLIST | 12 |
| Strategy: Understand the Data | 12 |
| PRODUCTION CHECKLIST | 13 |
| Strategy: Quality Control..... | 13 |
| ABOUT..... | 14 |

INTRODUCTION

Litigation is complex, dynamic, and unpredictable. A good checklist is designed to be your guide in forming a consistent, repeatable process. From the moment litigation becomes imminent until a settlement or judgment, practitioners cannot afford to miss anything. Because of the high stakes of litigation, it is crucial to meet the necessary requirements to the court and zealously represent your client while managing time, budget, and risk. This manifesto will serve as a complete e-discovery checklist covering the legal discovery process.

The traditional Electronic Discovery Reference Model (EDRM) was developed in 2005 to provide practitioners with a common framework for work in e-discovery. Today, smaller teams are tackling e-discovery projects and “do-it-yourself” solutions are available at affordable rates for the small to medium case. At the same time, practitioners in e-discovery are expected to be technologically competent while the technology itself continues to evolve.

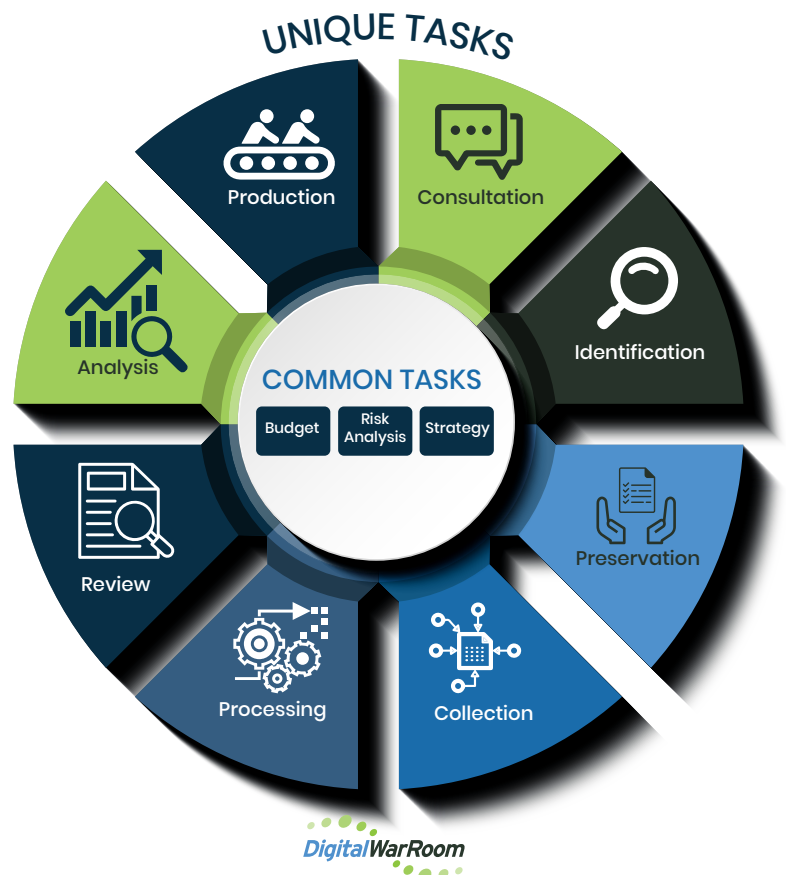
Educational content must also evolve to encompass new technological requirements of practitioners in alignment with their traditional role of risk management, cost management, and time management. The authors recognize that these responsibilities constitute an iterative, nonlinear process. In this manifesto, we establish a comprehensive list of points which form a more accurate depiction of the e-discovery lifecycle for the modern-day practitioner.

THE E-DISCOVERY CHECKLIST MANIFESTO DIAGRAM

The diagram below is based in part on the EDRM diagram. The outer circle represents unique steps while the inner circle represents more common steps which may occur at any point in the process. Like the EDRM, this is not a literal, linear or waterfall model. The order of the stages are only important conceptually. In reality, practitioners can cycle back to earlier steps at any time, refining their approach to gain a better understanding of the data or as the nature of the matter changes. The diagram is intended for discussion purposes, not as a prescription for the one and only right way to approach e-discovery.

It is necessary, too, that strategic planning, cost, and risk management play a role in the e-discovery process. Included in the diagram below are recommended strategies, budget, and risk management techniques that will enhance the use of the checklists.

Given this context, all stages outlined in the diagram should be considered at one or multiple points as practitioners move through an e-discovery project. The goal of the checklist manifesto is to include a checklist associated with each stage.





CONSULTATION

There are legal issues and obligations that every practitioner should be aware of that guide the e-discovery process. It is not necessary to know or to cite chapter and verse of the federal or applicable state rules, but practitioners will need to have a basic understanding of civil procedure rules on the federal level or the state law equivalents.

FEDERAL RULES: THE FEDERAL RULES OF CIVIL PROCEDURE (FRCP)

Rule 1: Just, Speedy, and Inexpensive

- The FRCP should be utilized in manner to secure the just, speedy, and inexpensive determination of every action and proceeding.

Rule 11: Signing Pleadings, Motions and Representations to the Court

- An attorney must sign every pleading, motion or other paper and certify it is the document is not presented for any improper purpose, that it pertains to the claims and defenses in the case and any factual contentions have evidentiary support

Rule 26(a): Initial Disclosures

- Parties must automatically disclose, without a request, names of individuals who have discoverable information, a copy of or description of ESI supporting claims or defenses, a computation of damages claimed

Rule 26(b): Scope and Proportionality

- Parties may obtain discovery of “any nonprivileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case.”
- “Information within the scope of discovery need not be admissible in evidence to be discoverable”
- A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost

Rule 26(f): Conference of the Parties; Planning for Discovery

- In conferring, the parties must consider settlement, make or arrange for ESI disclosures; discuss any issues about preserving discoverable information; and develop a proposed discovery plan

Rule 26(g): Signing Disclosures and Discovery Requests and Objections

- Attorney or party must sign discovery requests and objections and certify they are complete and correct, nonfrivolous, not used for any improper purpose, and not unreasonable, burdensome or expensive

Rule 34 - Form of Production and Specificity

- A party may serve on any other party a request for production of documents. This request must specify with reasonable particularity each item or category of items to be inspected.
- Any objection to a document request must “state with specificity the grounds for the objection.”
- The request must also specify the form in which ESI is to be produced
- Electronic documents will be produced as kept in the ordinary course of business or organized in categories responsive to a request
- Documents must be produced in a “reasonably usable form”

ABA Model Rule 1.1 on Duty of Competence

- Comment 8: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject

CLIENT MEETING CHECKLIST:

And there are additional consultation points that every practitioner should consider in initial discussions with the client. Client interviews should lay the foundation for Identification, Preservation and Collection, and the notion of information governance should be a discussion had with each client as well.

Consultation can occur at any time and should ideally occur before any specific litigation arises in order to adequately prepare the client in a proactive manner for issues that may arise should litigation occur. Consultation may then occur cyclically throughout any project and will flow into the strategy checklist set out further below.

Consider these points when litigation becomes imminent:

REVIEW OF FACTUAL ISSUES:

- ☐ Discuss with client the nature and substance of any imminent or actual legal claims and events leading to any claims
- ☐ Identify dates of occurrence
- ☐ Identify key people involved in events

INFORMATION GOVERNANCE CONSIDERATIONS:

- ☐ What are the document management systems (DMS)?
- ☐ Are there specific document types, technology and/or training of personnel common to the client's business and the employees who will be involved in this discussion?
- ☐ What systems for content creation exist?
- ☐ What hardware and software applications are in use?
- ☐ What is the current data management strategy?
- ☐ Does the client have any formal information governance or data retention policies and procedures?
- ☐ If so, what are they and what tools are used?
- ☐ If not, how do employees save, retrieve and share documents?
- ☐ What backup practices are in place?
- ☐ What documents fall under a legal requirement such as HIPPA, banking, privacy regulations, insurance, etc.?
- ☐ Does the IT department keep a data map? If not, they should.
- ☐ Can client provide a complete employee organizational chart with name, positions, business locations; all linked to the data map.
- ☐ Consider privacy considerations with HR people and discuss any and all document retention areas where privacy issues may apply
- ☐ Gather copies of all insurance coverage documents, including policies and analysis of coverage for disputes that may arise. Don't forget policies on individuals including life insurance policies that may have E/O or DI coverage.

STRATEGY: MANAGE EXPECTATIONS

A lawyer cannot provide a specific budget or pricing until the items in this checklist are considered and agreed upon. Wrap your checklist conclusions into a timeline with action items and Project Management items from the Strategy section. Managing and controlling the consultation from the outset is a clear strategic planning goal.

Budget: When budgeting in the consultation stage, practitioners need to consider the number of hours involved in conversations, meetings, and other interactions with the client and multiply those hours by applicable hourly rate to arrive at a projected cost.

Risk: The biggest risk in this early stage is potentially overlooking a significant source of potentially relevant data. It can be costly and time consuming to go back and perform re-work. Failure to identify or preserve relevant information can be costly as well.



IDENTIFICATION

The goal of Identification phase is to identify potentially relevant sources of ESI which could include people and systems. One common way to do this is to create a data map. The sources of ESI and custodian information will also be crucial to issuing an effective litigation hold in the Preservation stage. The scope of potentially relevant data may be uncertain in the early phases of a legal dispute, so after gathering insight from the initial client consultation and custodian interviews, the next step is to figure out where relevant data resides and who has custody or control of that data.

DATA MAP

A successful electronic discovery project should include an accurate picture of the target company's data sources. The data map will consist of all hardware and software deployed to accomplish routine tasks such as managing company email or creating data backups.

Data maps tend to vary widely from organization to organization and even within separate units of a large company. The identification process will locate servers of all types with data of all types (e.g. file servers, collaboration servers, email servers, web servers) as well as any data management systems (e.g., document management systems, financial systems, disaster recovery, and backup systems). The data map will also cover user-created data such as user home directories or departmental shared directories. It should also include BYOD (Bring Your Own Drive) sources such as laptops, tablets, smartphones, memory cards and access from home computers.

Many of the sources of ESI will likely be tethered to individual users, but as will be seen, there are non-custodial sources of ESI as well.

Here is a checklist of sources of potentially relevant ESI:

SOURCES OF ESI

- ☐ Email systems
- ☐ Text messaging systems
- ☐ Social media applications
- ☐ Websites and web servers
- ☐ Collaborative and messaging applications (e.g., Slack, Google Chat, Facebook Messenger, WhatsApp)
- ☐ File servers (departmental and personal directories)
- ☐ Voicemail systems
- ☐ Document management systems
- ☐ Cloud-based applications
- ☐ Databases
- ☐ Personal computers and laptops
- ☐ Mobile devices, smartphones and tablets
- ☐ External drives, flash media and network attached storage
- ☐ Home computers
- ☐ Backup systems
- ☐ Legacy systems
- ☐ Internet of Things (IoT) or connected devices

NON-CUSTODIAL SOURCES

- ☐ Marketing & sales information systems
- ☐ Product development, intellectual property and research (including notebooks, patents, R&D database, etc.)
- ☐ Human resource and personnel data (including HR policies and procedures)
- ☐ Document Management System (DMS) (including document naming conventions, how documents are saved and stored)
- ☐ Customer Service / Help Desk
- ☐ Finance, accounting and billing data
- ☐ Legal department
- ☐ IT department

CUSTODIANS

Organizations should also begin the identification process by identifying the key players or custodians involved in the events leading to any legal dispute. This requires some analysis of the following:

- ☐ Who are all the possible custodians?
- ☐ What is the reporting structure?
- ☐ Who has access to what data?
- ☐ What systems and applications do they use?
- ☐ How does each employee relate to each data source?

Another way to approach the issue of custodians is to cast a broader net and conduct individual custodian interviews. A custodian interview checklist would include at least the following inquiries:

- | | |
|--|---|
| <input type="checkbox"/> Name | <input type="checkbox"/> How do you manage your email? |
| <input type="checkbox"/> Title | <input type="checkbox"/> Do you use a personal device for work-related activities? |
| <input type="checkbox"/> Contact information | <input type="checkbox"/> Do you have a home computer with relevant information? |
| <input type="checkbox"/> Job description | <input type="checkbox"/> Do you have any paper documents that may be relevant? |
| <input type="checkbox"/> Predecessor | <input type="checkbox"/> Do you know anyone else who may have relevant information? |
| <input type="checkbox"/> Do you use a personal computer or laptop? | |
| <input type="checkbox"/> What software applications do you use? | |
| <input type="checkbox"/> Where do you save any potentially relevant documents? | |
| <input type="checkbox"/> Identify any folders, directories or other storage locations? | |

STRATEGY: PLAN FOR REASONABLENESS

The process of identifying ESI in discovery must be viewed under a microscope of reasonableness. That is the standard for testing whether the appropriate scope and steps were taken to identify ESI in litigation. Take reasonable and proportional steps to meet discovery obligations.

Budget: Much like the consultation stage, the budget in the identification stage will consist largely of the hours devoted to working with a client organization to identify the sources of potentially relevant ESI.

Risk: The risk of overlooking significant sources of ESI continues in the identification stage. That risk can be mitigated using the checklist above and thorough client meetings and comprehensive custodian interviews.



PRESERVATION

Identifying custodians and sources of ESI is where the process begins, but the underlying legal responsibility here is to isolate and protect against the intentional or unintentional destruction of potentially relevant data. This process must be reasonable; proportionate; efficient and auditable. The phrase often used by practitioners is that this should be a “repeatable, defensible process.”

The duty to preserve relevant data does not always flow from a litigation hold notice. It may arise under a common law obligation, a statute or regulation. In Federal court, the obligation arises when the party has received notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation. The failure to preserve relevant ESI can result in sanctions under certain circumstances.

Finally, remember that the duty to preserve is not the same as the directive to produce. Theoretically, preservation is broad while production is more targeted. Begin with your strategy and work forward from there.

A PRESERVATION CHECKLIST

- ☐ Confer with in-house/outside counsel and IT personnel
- ☐ Meet with and plan with IT and records personnel
- ☐ Determine the scope of duty to preserve
- ☐ Consider specific custodians and sources of ESI
- ☐ Is there a relevant time frame?
- ☐ Suspend any auto-delete or records disposition practices
- ☐ Review backup procedures and impact on preservation
- ☐ Determine if relevant ESI is reasonably accessible
- ☐ Consider proportionality to issues in the case
- ☐ Identify and mitigate any potential spoliation issues
- ☐ Consider departing employees or retiring of systems
- ☐ Sequester, lock or collect ESI and other information
- ☐ Contemplate additional custodial interviews

IMPLEMENT A LITIGATION HOLD

A litigation hold is a directive, usually in the form of a memorandum or letter, that directs individuals and leaders within an organization to preserve information and tangible items that may be relevant to a legal dispute, investigation or regulatory inquiry. Organizations might also need to put a litigation hold in place in response to an audit or subpoena.

Federal statutes and rules are silent on the requirement to implement a litigation hold. The obligation arises under the common law requirement that litigations preserve evidence. A litigation hold should be implemented any time an organization becomes aware of or reasonably anticipates litigation. That means, as soon as reasonably practicable upon notice of actual or imminent litigation, an organization should send a notice to the appropriate individuals directing them to preserve and not alter or delete any information that may be relevant to the subject matter.

A preservation letter is a slight variation on a litigation hold. An organization or law firm might send a preservation letter, for example, to another party or a third party to request that they preserve certain ESI.

A checklist for creating a litigation hold should include the following:

- ☐ A summary of the nature of the dispute, investigation or inquiry
- ☐ A statement of the organization's obligation to preserve potentially relevant information
- ☐ A statement that usual retention and disposition practices will be suspended
- ☐ A clear directive not to delete, alter or destroy any relevant information
- ☐ The sources of potentially relevant ESI and documents
- ☐ The types of ESI, documents or other materials to be preserved
- ☐ Instructions on how to handle potentially relevant ESI
- ☐ A section asking the recipient to acknowledge receipt of the hold notice
- ☐ The right person to contact if there are any questions
- ☐ An appropriately scoped distribution plan

STRATEGY: THOUGHTFUL AND REASONED APPROACH

Implementing a litigation hold does not end once the notice is sent. It is also necessary to track responses to the hold, follow up with custodians as needed, and to potentially add additional custodians and sources as the case develops. A litigation hold can be an iterative process and it may be necessary to monitor the status of the hold or issue periodic reminders to custodians. And finally, a litigation hold should eventually be released.

Budget: The budget related to preservation will revolve around the time and effort needed to physically preserve or segregate potentially relevant ESI and then draft and implement a litigation hold.

Risk: Failure to preserve is perhaps the greatest risk of any e-discovery project. If not properly preserved, data may be permanently lost. It is also the most frequent reason that courts impose sanctions.



COLLECTION

Collection is the acquisition of potentially relevant ESI, including files, graphics, images, data and any other form of digital information. Arguably the single most important aspect of collection is understanding how the ESI will later be used and collecting the data in a way that best facilitates that use and the specific needs of the case.

Generally, how ESI is collected will impact each successive stage of an e-discovery project. Therefore, it is necessary to first decide how the data will be collected.

FORMS OF COLLECTION

- **Full forensic collection** – this is a formal and highly technical process that results in a forensically sound, bit-for-bit copy of a data source (e.g., computer hard drive, server or other media).
- **Targeted collection** – this involves collecting only selected ESI from specific locations on a hard drive, server or other data source. A write-protecting hardware or software is used in a targeted collection to prevent the alteration of metadata during the collection process and each file is assigned a hash value to validate that it has not been altered during collection.
- **Self-collection** – this typically involves using informal tools to simply copy files and other ESI from one location to another. This process might be used in less formal circumstances where strict rules of authentication and the admissibility of evidence may not apply and where there is no need for forensic collection.

There are many sources of potentially relevant ESI and varying methodologies for collecting that data. However, in most instances, collecting user created content, whether it consists of email, word processing or spreadsheet files, or even backup media, will deploy one of the three methods outlined above to collect the ESI. Even collecting web-based and social media data is typically conducted in a forensic, targeted or informal manner. The best practice is to base the collection on the needs of the case.

COLLECTION CHECKLIST

- | | |
|---|--|
| <input type="checkbox"/> Plan and determine final scope of the collection | <input type="checkbox"/> Confer with IT personnel regarding access to data sources |
| <input type="checkbox"/> Prepare list of custodians and data sources | <input type="checkbox"/> Confirm and schedule collection |
| <input type="checkbox"/> Determine collection type | <input type="checkbox"/> Perform collection and validation of ESI |
| <input type="checkbox"/> Determine resources, tools and techniques for collection | <input type="checkbox"/> Prepare/obtain acquisition report/collection log |
| <input type="checkbox"/> Engage resources to perform collection | <input type="checkbox"/> Initiate/obtain chain of custody documentation |
| <input type="checkbox"/> Create collection specification/statement of work | <input type="checkbox"/> Prepare a status report for legal team |

STRATEGY: BASE COLLECTION ON THE NEEDS OF THE CASE

If ESI is not properly collected, it can have serious implications later in the case. It is best to focus a collection on relevant custodians and sources of ESI and to focus on how the data will be filtered and culled in the next step, processing.

Budget: The cost of a collection necessarily depends on the type of collection the volume of the data and the resources used to perform the collection. While deploying teams of forensic examiners to perform extensive collection is going to be costly, there are tools and technologies that may be deployed to make collection less costly. Again, focus on the needs of the case.

Risk: Potential pitfalls in collection include poor or improper collection techniques that may result in spoliation of data. Other risks include failure to properly catalog and validate that ESI has been collected properly to ensure metadata has been preserved.



PROCESSING

After collection, it is necessary to “process” data to prepare it for review. The bulk of this stage is usually carried out as you add or upload collections into an e-discovery software platform. The goals of processing are to first identify what is in the data set and then to develop processes for filtering and culling the ESI to arrive at those documents that will be promoted for actual review. To enable defensible reduction of data, practitioners will create filter criteria, such as a relevant date range, search terms or file type filters, which will carry only appropriate documents forward for review.

WHAT HAPPENS DURING PROCESSING?

- **Extraction of metadata:** Fields of data consisting of the attributes and properties of electronic documents are extracted.
- **Indexing of text:** All text in your documents will be extracted and indexed so that the text is searchable.
- **Exceptions:** Documents that could not be opened during processing will be reviewed as exceptions.

A PROCESSING CHECKLIST:

The following checklist may be used to identify the primary tasks to be completed during the processing phase of an e-discovery project:

- | | |
|--|--|
| <input type="checkbox"/> Intake and catalog data for processing | <input type="checkbox"/> Identify and apply data filtering and culling techniques (date, keyword, de-NIST) |
| <input type="checkbox"/> Update chain of custody | <input type="checkbox"/> Determine de-duplication policy (global or limited, Full de-duplication or “Near-dupe”) |
| <input type="checkbox"/> Plan for and determine resources, tools, and techniques for processing | <input type="checkbox"/> Monitor and quality check processing output |
| <input type="checkbox"/> Confirm processing features and workflow (drag & drop, foldering, document ID numbering convention) | <input type="checkbox"/> Review exceptions/anomalies in processing |
| <input type="checkbox"/> Confirm output/deliverable format (i.e., review platform in use) | <input type="checkbox"/> Transfer data to document review database |
| <input type="checkbox"/> Engage resources to perform processing | <input type="checkbox"/> Perform quality checks on document review database |
| <input type="checkbox"/> Prepare processing specification documentation | <input type="checkbox"/> Update chain of custody |
| <input type="checkbox"/> Stage and prioritize data for processing | <input type="checkbox"/> Determine storage/disposition of client data |
| <input type="checkbox"/> Ingest, and process ESI | <input type="checkbox"/> Close processing/prepare status report for case team |

STRATEGY: REDUCE THE DATA SET

The principle reason for processing is to convert disparate forms of ESI into a uniform format for review. But another important objective in processing is to filter and cull the data to reduce the overall volume of the data.

Budget: eDiscovery vendors offer a range of pricing models. Consider if your chosen vendor charges processing fees, hosting fees or uses another method. The cost of processing (if any) is driven almost entirely by the volume of data. Be diligent, understand vendor pricing models, and consider options to reduce data volume and fees where possible. It is important to carefully control the identification, preservation and collection stages to ensure they are reasonable and proportional to the needs of the case. When budgeting, consider the volume of data to be processed and any professional services time associated with processing.

Risk: Several risks arise in processing that can be mitigating by employing a consistent process. Implementing quality control checkpoints as indicated in the checklist, ensuring the integrity of the output and monitoring processing exceptions are critical to a defensible processing workflow.



DOCUMENT REVIEW

Document review is where a legal team will likely spend most of its time during an e-discovery project. During review, the legal team will identify the documents that will be produced. Another objective during review is to identify documents that will be withheld on the basis of attorney-client privilege or the work product doctrine. Additionally, it is during review that documents may be categorized according to the relevant issues in the case.

REVIEWING TECHNIQUES ARE USED TO IDENTIFY:

- Responsive documents to produce
- Documents relevant to issues in the case
- Privileged documents to withhold

Keep in mind that 60-70% of the total cost of an e-discovery project will arise during the review process. It is the most expensive component of an e-discovery project because it is the most human-intensive. It is for these reasons that it is crucial to keep in mind during the early stages of your project what the downstream costs will be in terms of review. The more documents that need to be reviewed the more costly the review will be.

SOME STEPS TO CONSIDER TO MAXIMIZE EFFICIENCY AND ORGANIZE THE DOCUMENT REVIEW ARE:

- ☐ Gather relevant case documents
- ☐ Determine how documents will be coded (e.g., Responsive, Privileged, Issue Codes, etc.)
- ☐ Prepare a review memorandum to guide the review team
- ☐ Develop a quality control policy

The following checklist may be used to identify the primary tasks to be completed during the document review phase of an e-discovery project:

- | | |
|---|--|
| <input type="checkbox"/> Meet with case team to plan document review process | <input type="checkbox"/> Perform first-level document review |
| <input type="checkbox"/> Prepare document review protocol and gather key case documents | <input type="checkbox"/> Perform second-pass document review |
| <input type="checkbox"/> Determine resources, tools, and techniques required for review | <input type="checkbox"/> Perform privilege review |
| <input type="checkbox"/> Engage resources required for review | <input type="checkbox"/> Perform technology-assisted review |
| <input type="checkbox"/> Determine linear manual review vs. technology-assisted review | <input type="checkbox"/> Apply redactions to documents |
| <input type="checkbox"/> Prepare review attorney/contract attorney roster | <input type="checkbox"/> Monitor progress of document review; report as needed |
| <input type="checkbox"/> Batch documents and prioritize for review | <input type="checkbox"/> Perform quality control on documents reviewed; report as needed |
| <input type="checkbox"/> Train the review team and brief them on the issues in the case | <input type="checkbox"/> Assist to prepare privilege and/or redaction log |
| | <input type="checkbox"/> Close document review; prepare status report for case team |

STRATEGY: CONSISTENCY

One of the most important things a document review team can do is be consistent. Consistency is not always easy to achieve in document review. It is dependent upon having a sound, efficient process that is clearly understood by the review team.

Budget: Budgeting for document review involves mostly consideration of the volume of the documents to be reviewed and the number of people involved in the review of documents. It is possible to roughly estimate the number of hours required, but there are variables such as the complexity and density of the documents that may not yield a reliable result. In the end, it's the hourly cost of reviewers multiplied by the volume of documents reviewed per hour.

Risk: There's tremendous risk associated with document review because it is the point in the e-discovery process where decisions will be made to produce a client's documents to opposing counsel. Care must be taken to ensure there are quality checks in the review process to prevent privileged material from being produced and to make sure the relevant documents are identified.



ANALYSIS CHECKLIST

In the EDRM, the term “Analyze” refers to the process of understanding your data. It was function of the Review process. In contrast to the modular setup of the EDRM, it is best to take steps to understand your data at every step of the project, rather than confining analysis to a specific stage as the correct time to learn more about your data.

Still, document review provides essentially the last opportunity to analyze documents prior to production. As documents are reviewed, the review team will begin to understand the facts that can be drawn from the documents. It is important to have a plan for harnessing those facts and matching them to the legal issues, claims and defenses in a case.

The following checklist may be used to identify the primary tasks to be completed during the analysis phase of an e-discovery project:

- ☐ Which custodians possess relevant documents?
- ☐ What are the primary types of responsive documents?
- ☐ What dates are emerging as significant?
- ☐ Are there any date gaps in the documents?
- ☐ Are particular words, phrases, events important?
- ☐ Is there a need to categorize documents in a particular manner?
- ☐ Are certain custodians communicating with others?
- ☐ Have additional relevant custodians begun to emerge?
- ☐ Are written communications ending abruptly?
- ☐ Are documents confirming the facts or legal claims of your case?
- ☐ Are documents undermining facts or legal claims in your case?
- ☐ Do any documents influence motion or settlement strategy?
- ☐ Review team productivity metrics and reports
- ☐ Expenses vs. budget

STRATEGY: UNDERSTAND THE DATA

The whole point of discovery is to understand the facts and circumstances of the case. During the analysis stage, it is important to gain a full understanding of the data and how it may be used to support the story that needs to be presented.

Budget: The budget here will involve attorney and stakeholder time associated with gaining a more complete understanding the documents in the case.

Risk: Depending upon how you approach analysis, the risks here can vary widely. At the same time that a legal team is preparing to produce relevant documents, it is important to also identify documents that support the client's position. One recommendation is to begin identifying key documents and categorizing documents by issues in the case.



PRODUCTION CHECKLIST

At some point, either after the document review, or sometimes during the document review, it will become necessary to produce documents. This requires the preparation of any responsive, non-privileged documents for export and delivery to the other parties in the case. Since the production of documents typically involves transmitting a client's documents to an opposing party, is necessary to take precautions when preparing a production. Quality control checks at several points in the process will mitigate most concerns.

Production formats continue to be an issue, and it is important to specifically discuss and agree upon the form of production early in the case.

The following checklist may be used to identify the primary tasks to be completed during the production phase of an e-discovery project:

- ☐ Meet with legal team to plan and schedule production
- ☐ Determine format, tools, and techniques for production
- ☐ Prepare production specification documentation
- ☐ Request or send a sample load file to opposing party
- ☐ Engage resources required for production
- ☐ Perform inconsistent tagging and document family conflict check
- ☐ Generate TIFF images (aka imaging or conversion)
- ☐ Apply Endorsements
- ☐ Select metadata fields for export
- ☐ Export native files, TIFF Images, data fields and text in required format
- ☐ Deliver production to legal team for quality check
- ☐ Perform quality checks of exported data, text, and images
- ☐ Prepare deliverable media
- ☐ Perform quality checks of deliverable media
- ☐ Prepare/update document production log
- ☐ Deliver production using agreed-upon delivery method
- ☐ Assist to prepare/update privilege and/or redaction logs

STRATEGY: QUALITY CONTROL

Because document production is the point at which a client's documents are delivered to opposing counsel, the best strategy in this stage is one of quality control to ensure that only the right documents are produced.

Budget: The costs here will be the time and resources to export the production.

Risk: There are huge risks associated with giving a client's documents to opposing counsel. The checklist and quality control checks will mitigate these risks.



ABOUT DIGITAL WARROOM

Digital WarRoom offers a comprehensive toolset to process, review and produce electronic documents for e-Discovery. Founded in 2002, Digital WarRoom eventually grew out of its original role as a service provider, developing and commercializing Digital WarRoom e-Discovery software to be used by law firms in-house. Digital WarRoom brings competitive e-Discovery costs and price transparency, offering a hosted subscription for under \$10/GB/Month, and DWR is one of the few vendors also offering an affordable on-premise option – available at \$1795/Year/License. Where Digital WarRoom shines is its expertise, and availability for training. With any hosted subscription, DWR guarantees 1 month of included onboarding via screenshare, on top of the unlimited email help desk.

For more information, visit www.digitalwarroom.com or contact us at info@digitalwarroom.com.



ABOUT ACEDS

The Association of Certified e-Discovery Specialists, part of leading legal education provider The BARBRI Group, is a global membership association committed to promoting and verifying eDiscovery skills and competence for organizations and individuals through training and certification, and is supported by ACEDS chapters around the world. The association's goal is to help professionals and organizations reduce the costs and risks associated with eDiscovery, and realize the advantages of performing it effectively. ACEDS awards the Certified e-Discovery Specialist (CEDS) credential, which is held by practitioners at Am Law 200 firms, government agencies, including the U.S. Securities and Exchange Commission and United Nations, and some of the largest multinational corporations in the world.

For more information visit www.aceds.org or contact us at sales@aceds.org.



ACEDS

DigitalWarRoom

ACEDS.ORG

©2020 Digital War Room & Association Of Certified e-Discovery Specialists