Practical eDiscovery

Why you should understand eDiscovery and how you can manage it defensibly.

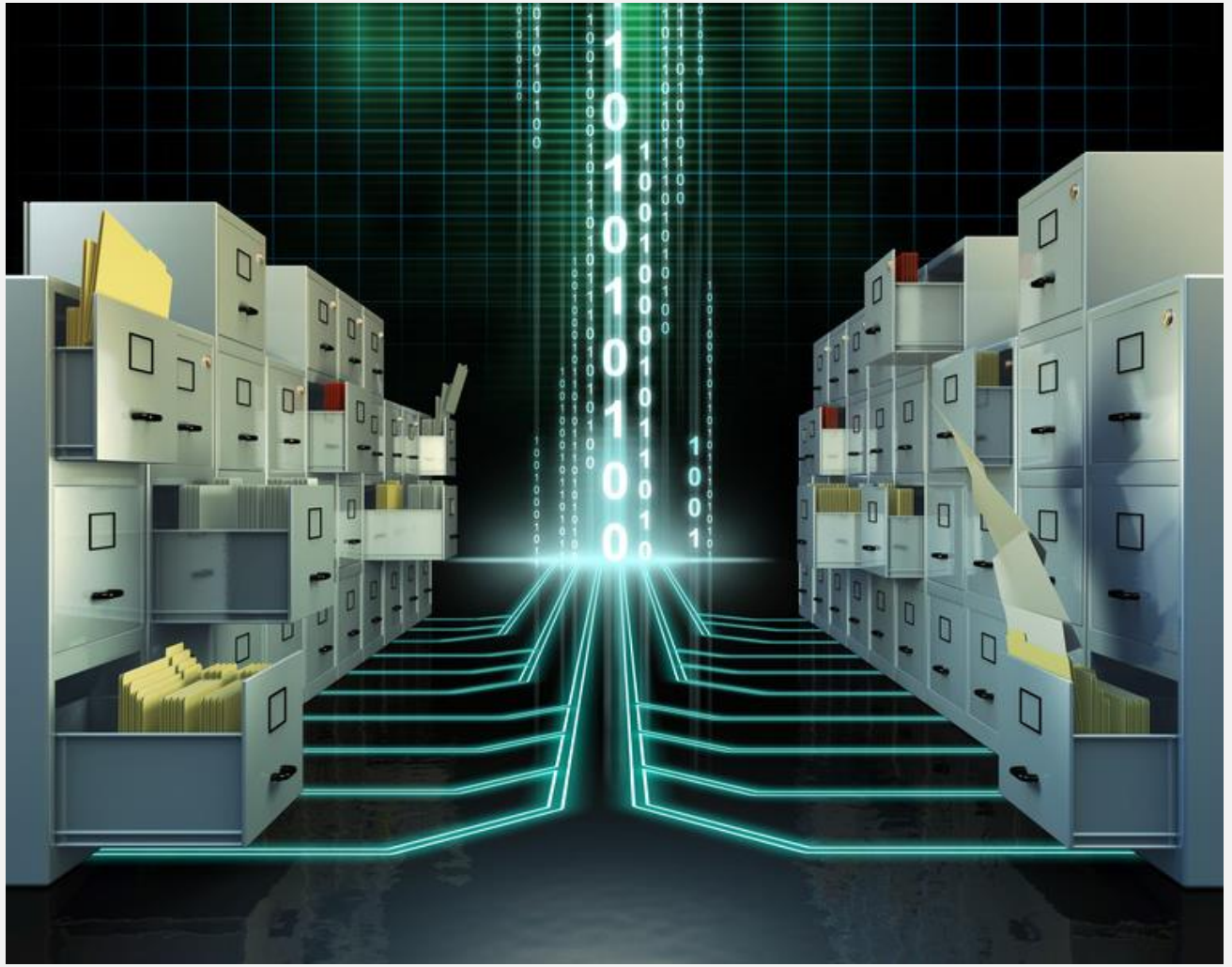
Presented by:
Kym Wellons, CEO
Sam Lewis, CTO

ESI can’t be ignored

Paper documents are no longer the way we live our lives or conduct our businesses.

We live in an age of digital transformation where the goal of many people and businesses is to become paperless.

As lawyers, we must be knowledgeable of and conversant in electronically stored information (ESI) and eDiscovery.



Ethics and eDiscovery

- Competent Representation
- Failure to Preserve and Spoliation
- Protection of Privileged ESI

RDi RESEARCH DATA INC

Competent Representation

- Rule 1.1 of the ABA Model Rules of Professional Responsibility
  - “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”
    - “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.” Comment 8.
- In 2016 Virginia amended Comment 6 to Rule 1.1
  - **The amendments effective March 1, 2016**, added the language “in the areas of practice in which the lawyer is engaged. Attention should be paid to the benefits and risks associated with relevant technology.”
- Many other states have adopted this language, or similar, in their own state ethics rules.

CA case study

- The relationship between e-discovery and the competent practice of law grows stronger each year.
- The State Bar of California Standing Committee on Professional Responsibility and Conduct Formal Opinion No. 2015-193:

> "An attorney lacking the required competence for the e-discovery issues in the case at issue has three options:
>
> 1) acquire sufficient learning and skill before performance is required;
>
> 2) associate with or consult technical consultants or competent counsel; or
>
> 3) decline the client representation.
>
> Lack of competent in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality."

CA case study

- Issues in the opinion's hypothetical:
  - "[A]ttorney made no assessment of the case's e-discovery needs or of his own capabilities..."
  - "Attorney exacerbated the situation by not consulting with another attorney or an e-discovery expert prior to agreeing to an e-discovery plan…"
  - "Attorney participated in preparing joint e-discovery search terms without experience or expert consultation and he did not fully understand the danger of overbreadth in the agreed upon search terms."
  - "At the least, Attorney risked breaching his duty of competence when he failed at the outset of the case to perform a timely e-discovery evaluation."

What does “competence” require?

- Attorneys handling eDiscovery should have familiarity and skill (either alone or supported for consultants or co-counsel) to:
  - Assess eDiscovery needs and issues
  - Preserve ESI appropriately
  - Analyze and understand a client’s ESI systems and storage
  - Identify custodians of relevant ESI
  - Perform appropriate searches
  - Collect responsive ESI in a manner that preserves the integrity of the ESI
  - Advise the client on options for collection and preservation
  - Engage in competent and meaningful meet and confer
  - Produce ESI in a recognized and appropriate manner

  (citing *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities*, LLC, 685 F.Supp.2d 456, 462-465 (S.D.N.Y. 2010).

RDi RESEARCH DATA INC

What do you think?

You represent a plaintiff in a wrongful death case brought after his wife was injured in a fatal car crash. You realize that your client's social media might be a problem after you see a post with a photo of your client in a t-shirt "I ♥ Hot Moms."

You ask your paralegal to direct the client to "clean up" his Facebook account because "we don't want blowups of this stuff at trial."

He deletes the posts and photos and closes his account.

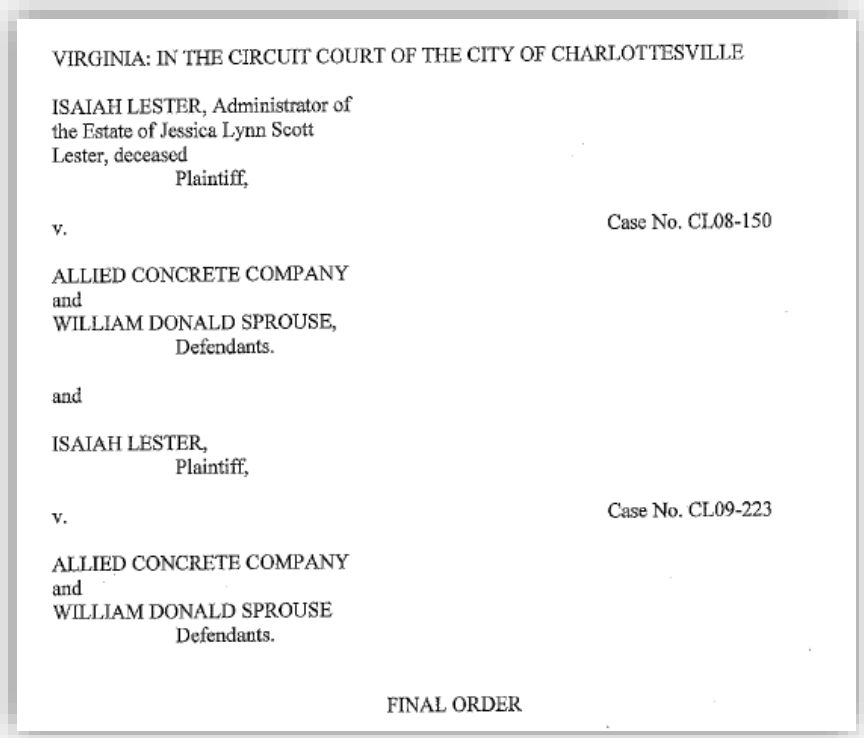
Is that a problem?

(c) Can Stock Photo / HypnoCreative

RDi RESEARCH DATA INC

What a Va. judge thought

- (Charlottesville, VA 2011) Judge Edward Hogshire's final order directed the payment of fees and expenses of $722,000 divided between the lawyer ($542k) and his client ($180k).
- Court found violations of:
  - Deceptive answer to discovery (Va. Sup. Ct. R. 4:1(g))
  - Spoliation and false representations to the court, failing to identify document on privilege log and failing to submit for *in camera* inspection.
    - Adverse inference instruction on one of the photographs that could not be recovered. Others were ultimately made available for presentation at trial.



VIRGINIA: IN THE CIRCUIT COURT OF THE CITY OF CHARLOTTESVILLE

ISAIAH LESTER, Administrator of
the Estate of Jessica Lynn Scott
Lester, deceased
Plaintiff,

v. Case No. CL08-150

ALLIED CONCRETE COMPANY
and
WILLIAM DONALD SPROUSE,
Defendants.

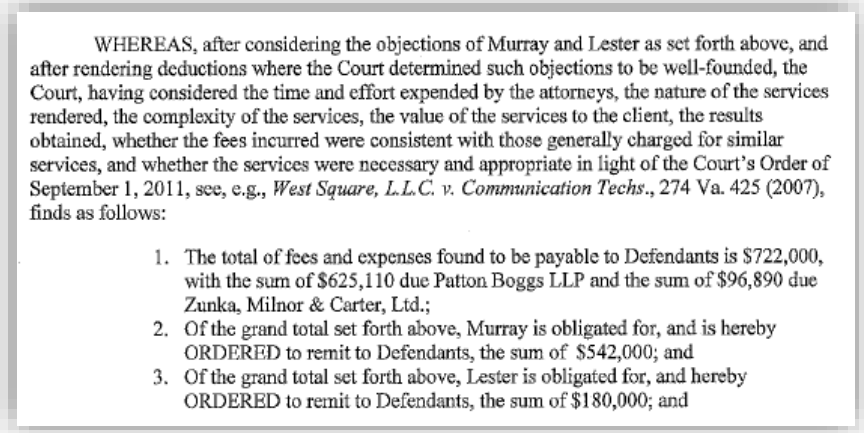
and

ISAIAH LESTER,
Plaintiff,

v. Case No. CL09-223

ALLIED CONCRETE COMPANY
and
WILLIAM DONALD SPROUSE
Defendants.

FINAL ORDER



WHEREAS, after considering the objections of Murray and Lester as set forth above, and after rendering deductions where the Court determined such objections to be well-founded, the Court, having considered the time and effort expended by the attorneys, the nature of the services rendered, the complexity of the services, the value of the services to the client, the results obtained, whether the fees incurred were consistent with those generally charged for similar services, and whether the services were necessary and appropriate in light of the Court's Order of September 1, 2011, see, e.g., *West Square, L.L.C. v. Communication Techs.*, 274 Va. 425 (2007), finds as follows:

1. The total of fees and expenses found to be payable to Defendants is $722,000, with the sum of $625,110 due Patton Boggs LLP and the sum of $96,890 due Zunka, Milnor & Carter, Ltd.;
2. Of the grand total set forth above, Murray is obligated for, and is hereby ORDERED to remit to Defendants, the sum of $542,000; and
3. Of the grand total set forth above, Lester is obligated for, and hereby ORDERED to remit to Defendants, the sum of $180,000; and

RDi RESEARCH DATA INC

Recent cases continue the trend

- Bellamy v. Wal-Mart Stores, Texas, LLC., 2019 WL 3936992 (W.D. Tex. 2019)
  - Defense counsel sanctioned to pay costs related to failure to disclose the known existence of a video that had been requested but which was lost and stating repeatedly that the video did not exist.
    - Court found no “bad faith” due to testimony that the file transitioned from an attorney who left the firm and the new attorney was unaware of the video’s existence.
    - Wal-Mart store manager requested that the tape be preserved and it was sent to the claims manager but went missing in transit, it appears.
    - “Defendant’s and its counsel’s mistakes were failing to be upfront with the loss of the video.”
    - “Rather than complying with the rules, defense counsel delayed the production of adverse material and the identify of witnesses and the extent of the inappropriate acts only fully became revealed after an inadvertent production of emails was made (after intervention by the Magistrate Judge).
      - See later discussion of 502(d) orders, which Defendant did not use in this case.

Recent cases continue the trend

- GN Netcom, Inc. v. Plantronics, Inc., No. 18-1287 (3rd Cir. 2019)
  - Refused to overturn district court's decision to punish conduct with punitive sanctions and costs along with instructions in lieu of dismissal. Monetary sanctions totally in excess of $5M.
  - Company's Sr. VP Sales sent email "Given the sensitive nature of this issue and the ongoing legal issues. Please delete this entire string of emails for everyone that has been copied ASAP!" He also deleted his own emails for a total of 40% of his emails during a ten-month period.
  - Plantronics' repeatedly obfuscated the mail deletion and acted in bad faith to impair the ability of the other side to effectively litigate its case.
- Klipsch Group, Inc. v. EPRO E-Commerce Ltd., No. 16-3636-cv, 16-3726-cv (2nd Cir. 2017)
  - $2.7M sanction for failing to place legal hold on a substantial amount of electronic data, including emails and faxes. After retaining an eDiscovery vendor, it produced an additional 40k documents. Even after an order from the Magistrate, documents were not produced and there was no adequate legal hold, documents were deleted and employees used data-wiping programs.

Failure to preserve

- ABA Model Rule 3.4 Fairness to Opposing Party & Counsel
  - A lawyer shall not (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act.
  - (d) in pretrial procedure … fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party.
- Va. Rule of Professional Conduct 3.4
  - The Virginia rule is not exactly the ABA rule
    - (a) There is no reference to "unlawfully" and states that the action is "for the purpose of obstructing a party's access to evidence."
    - (d) is actually (e) in the Virginia rule but the same language
  - Comments to the rule indicate that the intent is to foster "fair competition" and focuses on the procedural right to obtain evidence through discovery. It specifically notes the application of (a) to computerized information.

Spoliation

- Spoliation is the destruction or significant alteration of evidence or the failure to preserve properly for another's use as evidence in pending or reasonably foreseeable litigation.
- Spoliation can result in serious consequences:
  - Adverse inference
  - Dismissal
  - Separate cause of action for damages
- Attorneys have an obligation to explain to clients the consequences of spoliation both when litigation is pending and, often, when no litigation is currently pending.
- Attorneys have an obligation during the pendency of a case not to spoliate evidence.

Protection of Privileged ESI

- ABA Rule 1.6
  - An attorney has a duty to protect confidential communications between an attorney and his client and must take reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
- Sedona Conference Commentary on Protection of Privileged ESI (Nov. 2014) argued for more effective use of Rule 502(d).
- What is 502(d)?
  - Rule 502 generally provides that the "federal court may order that the privilege or protection is not waived by disclosure connected with litigation pending before the court – in which even the disclosure is not a waiver in any other federal or state proceeding."
  - A party agreement is not effective unless incorporated into a court order.

General Failure to Use 502(d)

- A 2015 Exterro Survey of judges found that 45% of judges polled reported that the biggest area where they believed parties could cut costs in litigation was with a privilege waiver under 502(d).
- 50% cited FRE 502(d) as the most underutilized e-discovery rule in their courtroom.
- The Sedona Conference also noted the failure of counsel to use the 502(d) order and attempted to “breathe life” back into 502(d).
- Some judges have suggested that failure to secure a 502(d) order is tantamount to malpractice.

Why Consider a 502(d) Order?

- A properly drafted order can address inadvertent waiver and intentional disclosure.
- Resulting in expedited discovery and cost savings.
- Potentially useful for limited disclosures of privileged communications.
  - For example producing document such as legal opinions substantiating reliance upon advice of counsel as an element of a cause of action.
- Any order should include:
  - Production is not a waiver of the privilege.
  - Be careful with “reasonable steps” language, production “whether inadvertent or otherwise” and specifically avoid any 502(b) analysis of reasonableness.
  - Use the word “inadvertent” carefully if you plan to protect intentionally produced documents.
  - Clawback process.
  - Procedures for privilege logs (if any).

But, be careful to object timely.

- There is a difference between *disclosure* and *use* of privileged information produced in litigation.
- Don't rely on a 502(d) order to support a non-waiver argument if you permit use of a document at deposition or in motion practice.
  - Certain Underwriters at Lloyd's, London v. Nat'l RR Passenger Corp, 2016 WL 6875968 (EDNY Nov. 17, 2016).
    - Amtrak produced thousands of documents pursuant to a 502(d) order. At deposition, plaintiff questioned deponent about documents containing work product designation. Amtrak reserved its right to object but never asserted a privileged objection. The next day, Amtrak asserted privilege and clawed back the documents.
    - Court found that while the 502(d) order applied to the disclosure, it did not apply to the use during deposition, which, if unopposed, could constitute waiver.

Why not use a 502(d) Order?

- Once privileged data is viewed by the other party, it potentially provides the other party with critical information.
  - Your adversary could use the information to pursue legitimate discovery
- A 502(d) order doesn't limit review obligations because you still have to conduct a detailed review of documents prior to discovery.
- Multi-jurisdictional litigation may present challenges because of overlapping (and inconsistent) state and federal rules.

eDiscovery Defensibility

- Reasonableness Standard
- General Protocol: EDRM
- Identify/Preserve/Collect
- Process/Review/Analyze
- Produce

RDi RESEARCH DATA INC

2015 Amendments to FRCP 26

- 2015 Amendments recognized the need to address the “serious new problems associated with vast amount of electronically stored information.” 2015 Year-End Report on the Federal Judiciary, Comments of Chief Justice Roberts.
- FRCP 26
  - Revised in 2006 (along with 16, 33, 34, 37 and 45) to include reference to ESI
  - Revised in 2015 to clarify scope and proportionality (largely a return to 1983 language)
  - Key input from Sedona Conference
    - Sedona Principles, Third Edition (October 2017) summary
      - The Sedona principles started in 2002 to serve as best practices, recommendations and principles for addressing EDI in disputes in federal or state court and during or before commencement of litigation.
      - Principles will be referenced throughout but can be found summarized at this link or in full text discussion on the Sedona Conference website.

2015 Amendments to FRCP 26

- Emphasis on:
  - Reasonableness and proportionality;
  - Cooperation among counsel to control expense and time demands of litigation;
  - Discouraging over-use, misuse and abuse of discovery regardless of the wealth or lack thereof of the party; and
  - Resolution between the parties preferred but call to judiciary to engage.

    "Judges must be willing to take on a stewardship role, managing their cases form the outset rather than allowing parties alone to dictate the scope of discovery and the pace of litigation." 2015 Year-End Report on the Federal Judiciary.

2015 Amendments to FRCP 26

- Recognition of developing technologies and approaches

  "Computer-based methods of searching such information continue to develop, particularly for cases involving large volumes of electronically stored information. Courts and parties should be willing to consider the opportunities for reducing the burden or expense of discovery as reliable means of searching electronically stored information become available." (Committee Notes, 2015)

(c) Can Stock Photo / SergeyNivens

RDi RESEARCH DATA INC

Practical Impact

- Relevance is broader than admissibility at trial.
- Requesting party has to prove relevance and the objecting party has to prove discovery is not proportionate.
  - Diminishing returns: when is discovery wasteful or unnecessary?
    - Importance of the issues
    - Amount in controversy
    - Relative access to relevant information
    - Resources -- prevent war of attrition or use as coercion
    - Importance of discovery to resolve issues
    - When does the burden outweigh the benefits
  - *See* Sedona Principle 2.

FRCP 26 and eDiscovery

- Key provisions
  - FRCP 26(b)(1)

    Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action , the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of discovery in resolving he issues and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

  - FRCP 26(b)(2)(B)

    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. On motion to compel, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

RDi RESEARCH DATA INC

FRCP 26 and eDiscovery

- FRCP 26(b)(2)(C)

  On motion on or its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

  (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

  (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or

  (iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1).

- FRCP 26(f)(3)

  A discovery plan must state the parties' view and proposals on:

  (B) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues;

  (C) Any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced.

FRCP 26 and eDiscovery

- FRCP 26(f)(3) cont.

  (D) Any issues about claims of privilege or of protection as trial-preparation materials, including – if the parties agree on a procedure to assert these claims after product – whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502.

- FRCP 26(g)

  Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney or record in the attorney's own name … By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

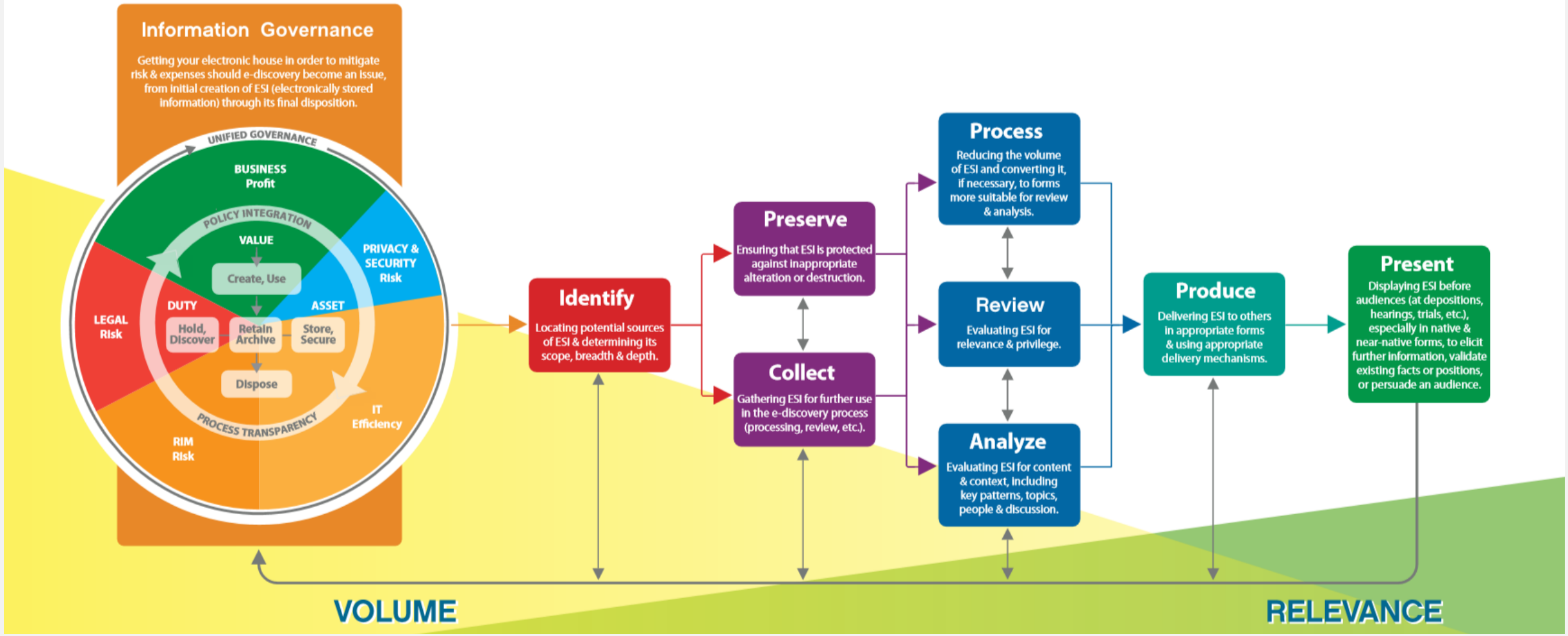
  (A) with respect to a disclosure, it is complete and correct as of the time it is made …

Electronic Discovery Reference Model

- EDRM is a recognized method of conducting defensible eDiscovery
  - Conceptual view – not literal, linear or waterfall
    - You may engage in some but not all of the steps or carry the steps out in a different order
  - Process is also iterative
    - You may repeat a step or series of steps multiple times or cycle back to earlier steps as you gain more knowledge of the data set
  - The model has evolved over time; history of the model is available on the EDRM website

Electronic Discovery Reference Model

Standards, Guidelines, and Practical Resources for Legal Professionals and E-Discovery Practitioners

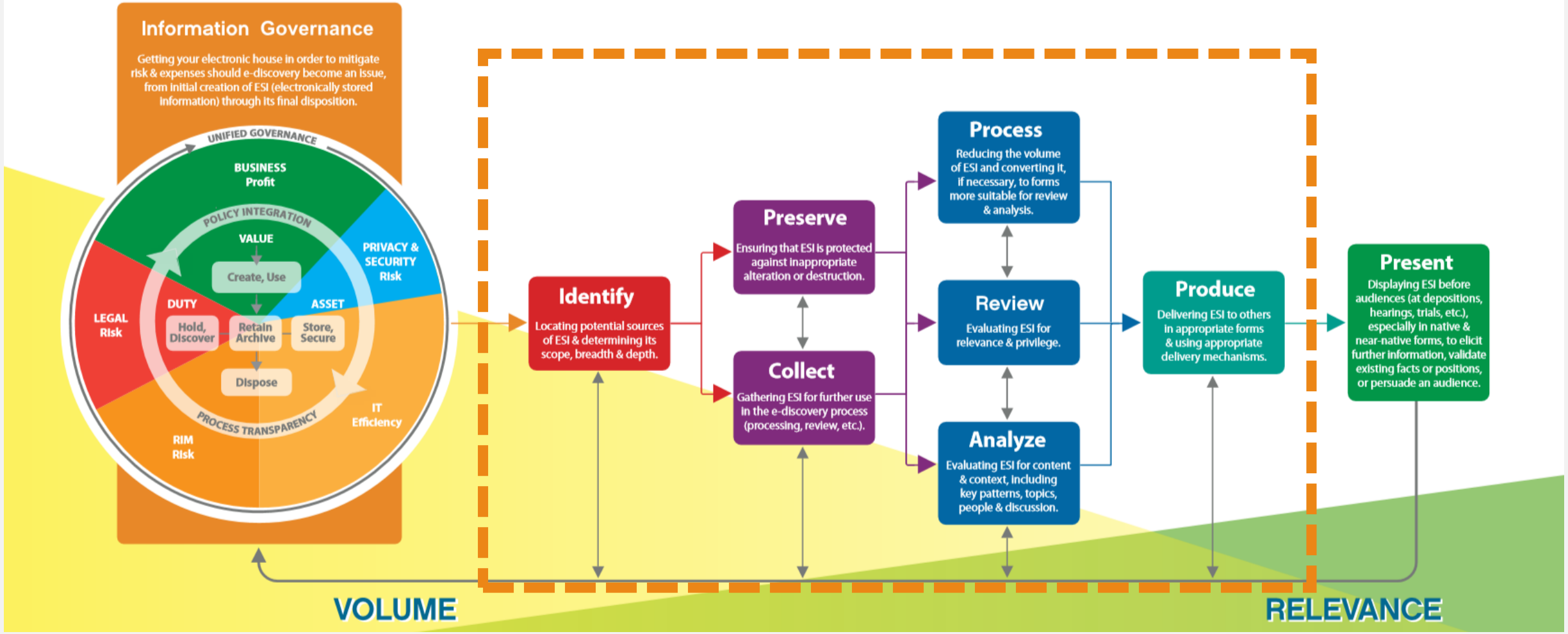


https://www.edrm.net/resources/frameworks-and-standards/edrm-model/edrm-wall-poster/

RDi RESEARCH DATA INC

Electronic Discovery Reference Model

Standards, Guidelines, and Practical Resources for Legal Professionals and E-Discovery Practitioners



https://www.edrm.net/resources/frameworks-and-standards/edrm-model/edrm-wall-poster/

RDi RESEARCH DATA INC

Identify

- You should define the information that might be relevant in the matter, required to respond to discovery and to prepare your case:
  - Review court disclosure requirements
  - Think ahead for likely discovery (affirmative and defensive)
  - Know your legal claims, proof and defenses (think jury instructions)
    - It is important to outline how each of you will approach the case, not just your perspective.
    - Equally important is to understand your affirmative case, not just your defense strategy.
    - What needle in the haystack are you looking for and which one are they looking for?
    - What time period is relevant?

Identify

- Identification involves identifying fact witnesses, but it also includes
  - Identification of systems and the owners of those systems;
  - Identification of practices around document and data storage, deletion, archiving, etc.; and
  - Identification of key players, such as IT, corporate counsel and eDiscovery vendors.
- Make lists
  - Know your claims so that you can determine relevant areas of inquiry and relevant time periods.
  - Identify individuals who possess or may have knowledge of relevant information.
  - Determine how each individual will be treated – custodian versus resource; key versus non-key witness.
  - How will you collect information? Survey, interview, combination?
  - Create a template for questions
    - Fact gathering
    - Data sources
    - Jargon, terms, business terms

Identify

- Technology has become such a part of everyday life that witnesses may not remember or recall a data source unless you specifically ask.
  - Walk a witness through his or her day and how they record and communicate information.
  - Discuss with them how they save, share, store and delete data.
  - Have lists to review with witnesses:
    - Common data types
    - Possibly relevant applications
    - Common storage vehicles

Common data and storage places…

RDi RESEARCH DATA INC

But what about???

Twitter Instagram LinkedIn YouTube Facebook

Microsoft | Office

VK Snapchat Facebook Messenger Pinterest

venmo

Identify

Survey or Interview the custodians.

Don’t just focus on facts of the case.

Make a concerted effort to talk with them about systems, protocols and practices both with hard copy and electronic data.

Ensure that you remind them of their obligation to preserve and what that means, include a clear understanding of the data sources and time periods.

Document the custodian responses.

Keep interview notes.

Retain all documents and document how and when received.

Maintain a master list of all custodians, interview date(s) and efforts to preserve and to collect.

Follow-up on leads.

Follow up on any additional custodians identified through the interview process.

Ensure that all new custodians are instructed to preserve and that you continue to interview until there are no new leads.

Don’t forget to follow up as new facts or theories emerge! That may introduce new sources of data.

Preserve: Legal Hold

- FRCP 37(e) requires preservation of evidence.
- Sedona Principle 5:

  “The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that is expected to be relevant to claims or defenses in reasonably anticipated or pending litigation. However, it is unreasonable to expect parties to take every conceivable step or disproportionate steps to preserve each instance of relevant electronically stored information.”

- Sedona Principle 7:

  “The requesting party has the burden on a motion to compel to show that the responding party’s steps to preserve and produce relevant electronically stored information were inadequate.”

- Sedona Principle 8:

  “The primary sources of electronically stored information to be preserved and produced should be those readily accessible in the ordinary course. Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is no longer proportional.”

Preserve: Legal Hold

- Duty to preserve data is triggered when “the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Zubalake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).
  - Demand letter
  - Formal complaint (verbal or written)
  - Regulatory proceeding (EEOC, DOL, etc.)
- Information preservation is an immediate requirement.
  - Identify who has information.
  - Discuss with your client the requirement to preserve.
  - Send preservation notices to:
    - People who possess information;
    - People who own the systems where information is stored; and
    - People who may have visibility to changes in custodian status.

Preserve: Legal Hold

- Litigation hold notice contents and methods
  - You should advise your client in writing to issue legal holds or do it yourself.
  - Legal hold notice should be written *in plain English*.
    - Ensure the notice describes the issue sufficiently for identification of relevant documents.
    - Provide examples of relevant information and sources
      - Specifically note assets under user control, such as cell phones, laptops, notebooks
    - Provide guidance for questions.
    - Explain the importance of the process.
    - Ask for identification of other witnesses.
    - Consider survey for other data sources or documents.
  - Document receipt
  - Plan for changes
  - Update periodically

Collect

Collection is not required for preservation… so, to collect or not to collect is the question.

Do you collect to preserve?

What is the risk of loss/spoliation?

Is there a planned change in systems that could impact collection?

What is the cost versus risk?

Do you collect in stages? Key versus non-key?

Collection from some but not all sources?

Do you collect for ECA?

Do you need to review the data to inform search terms and discovery planning/responsive pleadings/motion practice?

Do you trust your witnesses? Need to confirm key positions on the law or the facts?

Can you glean valuable insights from some but not all data sources?

Collect

- The preservation and collection of information must be proactively managed by the firm or company's staff attorney, along with eDiscovery and technical experts.
- Collection methods and considerations can be heavily influenced by the source of the data. Defensible collection methods will vary.
  - For example, email collection:
    - Back-end export from server or archive vs.
    - Front-end collection from email client with custodian
- Maintain a record of collection efforts
  - Track each custodian with their own folder when possible
  - Maintain dates of collection, method of collection and party responsible for collection
  - If you collect assets, maintain a chain of custody log
  - Always be able to go to the collection folder and answer collection questions
  - Separate by data type collected or data source

Collect: Cell phone and Social Media

- Evaluate decision to collect or not to collect carefully
  - Challenges in preservation
  - BYOD policies/personal data
  - Can be expensive
  - Collection requires credentials or physical access through custodian
- Requires specialized software to review
- Validation and spoliation risks

Collection and Proportionality

- With the rapid expansion of technology, you may have myriad sources of potential information about a matter that you could collect.
- It is critical to decide which sources are most relevant and which contain information the collection of which is proportional to its value in litigation.

This is a cycle. It may (likely will) happen many times over the life of a matter. Sometimes you will engage one or a combination.

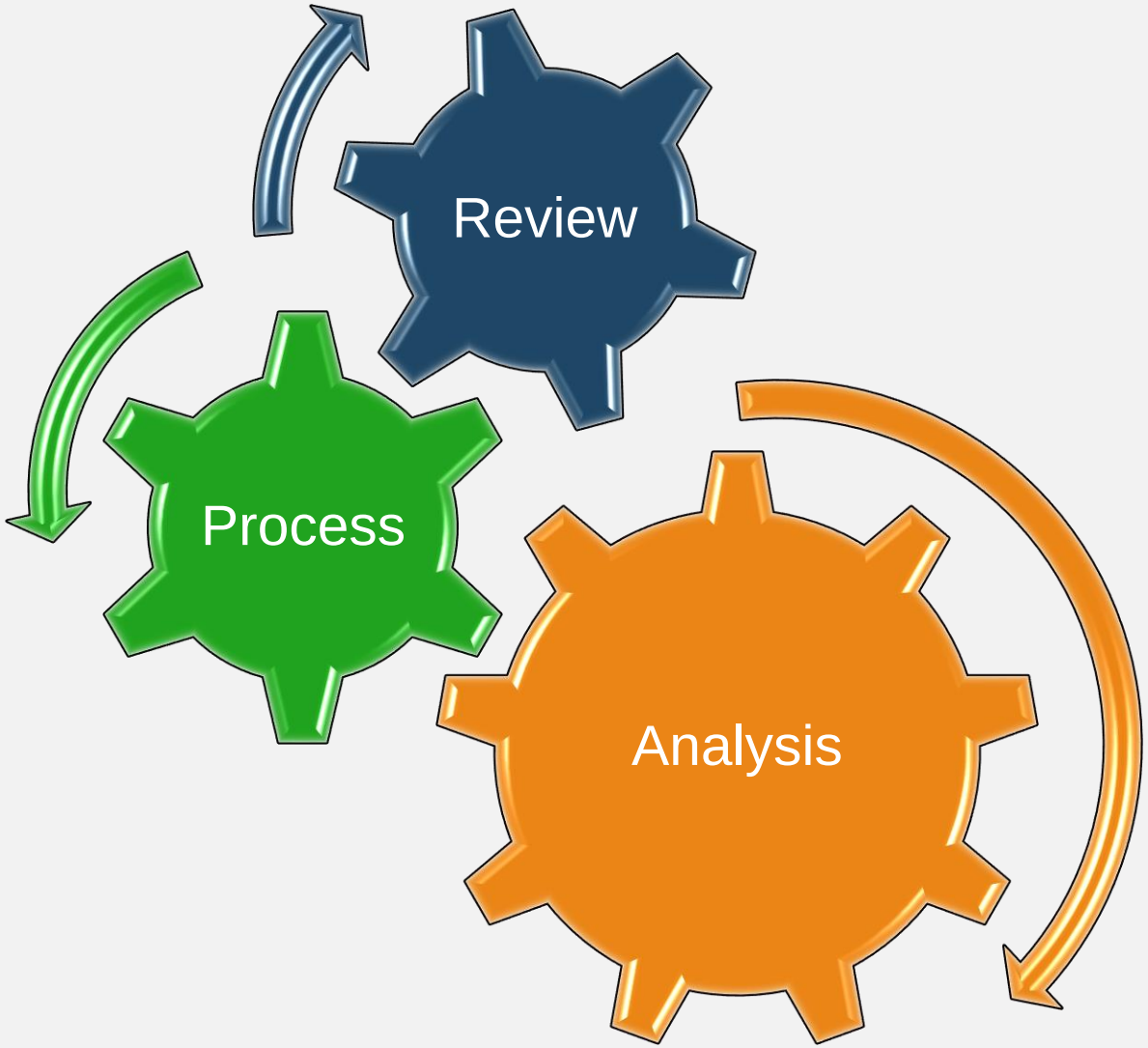
Process/Review/Produce

- Sedona Principle 6:

  “Responding parties are best situated to evaluate the procedures, methodologies and technologies appropriate for preserving and producing their own electronically stored information.”

- Sedona Principle 11:

  “A responding party may satisfy its good faith obligations to preserve and produce relevant electronically stored information by using technology and processes, such as sampling, searching or the use of selection criteria.”



This is a cycle with interrelated parts. Analysis should be an ongoing activity as you bring in data to process and as you review that data.

Process: Goals

- Record item level metadata
- Enable effective searching
- Enable effective review
- Enable defensible production

Process: Things to Think About

Processing of data involves:

- Assessing the data collected
- Preparing the data (sorting or organizing for ease of navigation and reporting)
- Validating output/handling exceptions
  - Data issues can delay review; often unknown until processing stage
- Documentation, QC/Validation and analysis of results

Review: Culling data

- De-Duplication, Near De-Duplication
- Use searching and analysis to remove extraneous or non-relevant data
  - Iterate search terms. Don’t just run searches and stop. You may have searches that are overly broad and picking up too much data. Revise them.
  - Accept diminishing returns. Focus your efforts on large data and don’t focus as much on removing small chunks of data.
- Consider Privilege. Can you run searches to identify potentially privileged documents, remove those for later review?
- Test your search sets, run statistical samples on the results that got excluded from your searches and the results that were included to verify your results.

Review: Plan for Reviewers

- Plan for a review; don’t just start reviewing.
  - Determine who will review which categories of documents/custodians
  - Evaluate bulk marking of certain documents
- Prepare your reviewers
  - Outline of case facts, law and arguments
  - Protective orders and confidentiality
  - Identification of key players, jargon and relevant relationships
  - Clear rules on marking, tagging, redacting, privilege, etc.; align for consistency
  - Ensure that you iterate training, if you have time.
  - Have subject matter experts available on site for questions/guidance.
- Establish immediate QC during training periods to catch issues quickly.
- Establish timeline goals and measure against those goals quickly.
- Plan for how you will use reviewed documents.

Analysis

- What are you seeing in your review sets?
- Are there patterns in your data?
  - Are you noticing daily reports that could be removed or bulk coded?
  - Are you noticing reference to a custodian who isn't in your collection set?
  - Are you noticing communications that seem to be referencing outside information, i.e. communications that seem incomplete or reference text messages
- Are you finding what you need?
- Don't wait until you are finished review to start this process! If you are not seeing what you want, consider going back and modifying your searches.
- Exploring gaps.
  - Did you expect to find communications between key custodians and there is nothing at all?

Produce

- Sedona Principle 12:

  “The production of electronically stored information should be made in the form or forms in which it is ordinarily maintained or that is reasonably usable given the nature of the electronically stored information and the proportional needs of the case.”

- Sedona Principle 13:

  “The costs of preserving and producing relevant and proportionate electronically stored information ordinarily should be borne by the responding party.”

Produce: General

- Don’t wait for production phase to think about production!
  - Create standard protocols for your matters
  - Evaluate the protocols for your matter
  - Technology changes, so should your standard protocols! Set a regular time to review protocols.
- Determine how documents will be produced
  - Factor in how you wish to produce AND how you wish to receive data.
  - Clearly communicate about load file formats.
- Think about rolling productions
  - Generally favored
    - Let opposing counsel know things are moving, particularly in bigger cases
    - Allows for iterative process to drive relevance and proportionality decisions

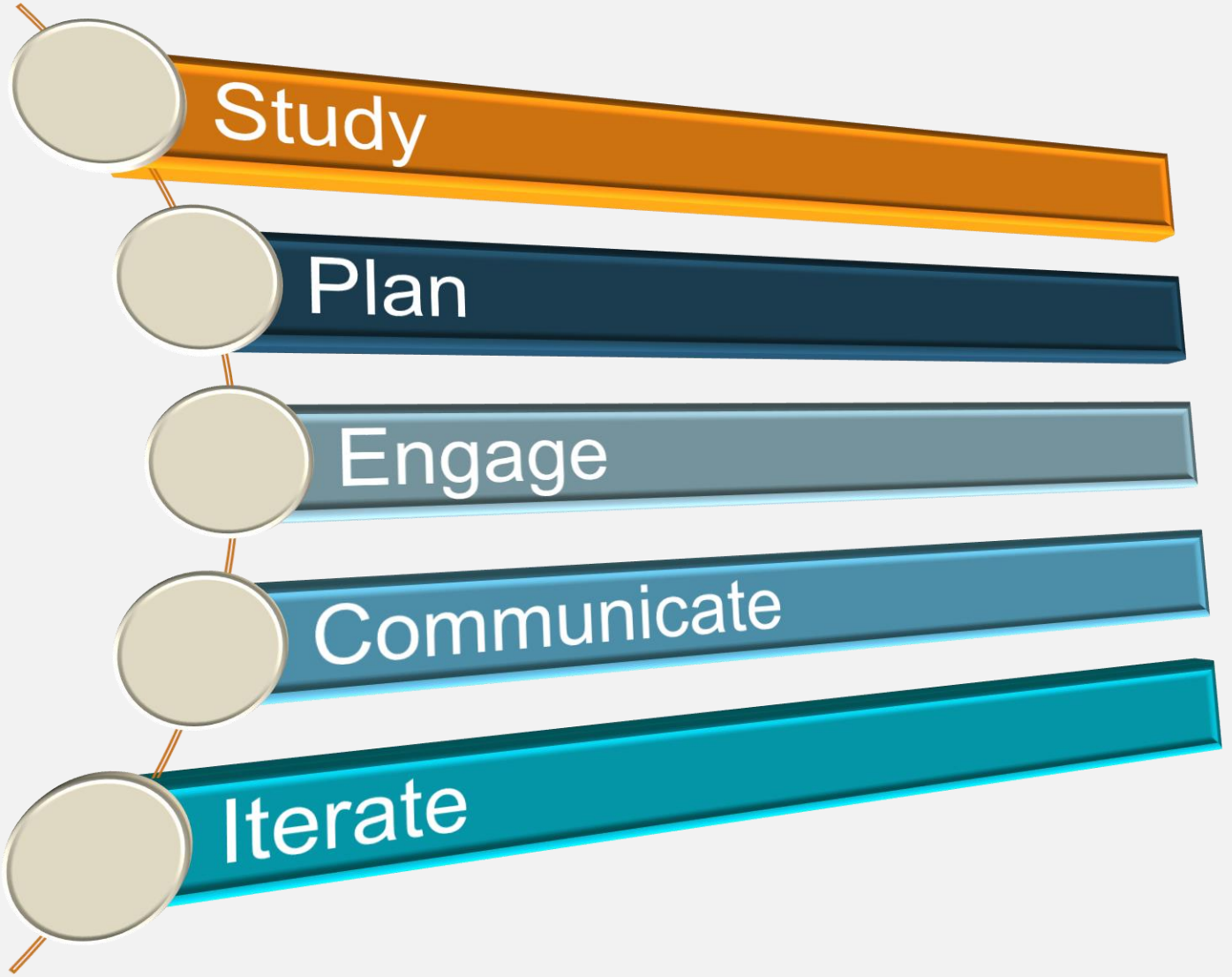
Produce: Common Forms

- General forms of production:
  - Native
  - Image (Near-paper)
  - Paper
  - PDFs
  - Images with Metadata
- Single page PDF versus single page TIFF

Produce: Things to Think About

- Threading
  - Best practice: review threaded, produce all.
  - Best practice for privilege log: one entry for each thread/one redacted document
- Metadata you need to ask for
  - BegDoc, EndDoc, BegAttach, EndAttach, Parent ID, Page Count, Author, From, To, CC, BCC, Email Subject, Custodian, DateSent, CreateDate, ModDate, Filename, Doc Ext, Filesize, Image Path, Text Path, Native Path (for documents with natives produced), Confidentiality (Optional)
- Red Flags
  - One PDF
  - PST
  - Lack of unitization

Key Themes



RDi RESEARCH DATA INC

QUESTIONS?