ISACA
Serving IT Governance Professionals
San Francisco Chapter

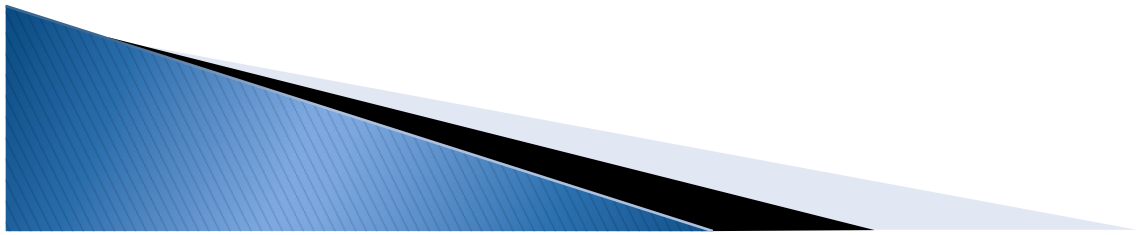
Electronic Discovery & Digital Forensics

Robert Schperberg

New
Federal Rule of Civil Procedures

Also Known As

"FRCP"



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Defining FRCP and ESI

- New Federal Rules of Civil Procedures was enacted December 1st, 2006
- The target of the new FRCP will be known as ESI (Electronic Stored Information)
- It will change the way businesses store digital information
- It will make digital stored information legally accessible

Reason for FRCP and ESI

- The new regulations, adopted by the U.S. Supreme Court in April, say businesses must be able to quickly find such data when required by the federal court.
- Every electronic document stored by businesses:
  - e-mail, instant messages, financials, voice mail and all text and graphical documents—must be easily retrievable.

What Does it Mean?

- "Lawyers aren't going to look at their caseloads and say, 'Well, this changes my whole approach.'
- But the new FRCP regulations will become a model for the way litigation is carried out in federal court—and eventually in state courts."
- For businesses, it means making changes in the technology used to store the information

What Does it Mean? (Continued)

- It will mean a lot of extra hours for staff that handles electronically stored information, because it means:
  - "We can't just save our data on tape or on disk anymore and make sure it's safe. We have to be able to get pretty granular about how to access it."
- The new regulations were part of an amended federal court rules the Supreme Court issued in April (Zubulake).
- Among them was a package of changes to the Federal Rules of Civil Procedure. Rules 26 and 34 through 37 cover the issue of e-discovery of critical evidence.

How Did We Get Here?

A Historical Perspective

- According to people involved in the move to get the rules adopted:
  - The match that lit all this was struck in March 2000, when then-Vice President Al Gore reported that he could not immediately produce e-mails related to a probe by the Department of Justice into his fund-raising activities.
  - At the time, White House counsel Beth Nolan said the White House e-mails were recorded on a series of 625 tapes that would take up to six months to be searched.
  - Setting up the tape-searching equipment alone would take two months, Nolan claimed

How Did We Get Here? (Continued)

- Shortly afterward, a movement was started to shore up the court rules in this area, led by Thomas Allman, senior counsel at the Chicago firm of Mayer, Brown, Rowe & Maw
- The 2003 Zubulake vs. UBS Warburg case added an extra push. In that case, the defendant (UBS Warburg) claimed that old, deleted e-mails requested by the plaintiff regarding a gender discrimination and retaliation dispute were stored on 94 separate backup tapes, and the cost of retrieving them $300,000--making the recovery of the information "unreasonable."

How Did We Get Here? (Continued)

- After several months of hearings, the court ultimately ruled that the plaintiff was to participate in the cost of restoration of the evidence, although the defendant was to bear the major part of the expense: UBS had to pay 75 percent and the plaintiff 25 percent of the cost of restoration.
- Also, the court ruled that the defendant must pay "for any costs incurred in reviewing the restored documents for privilege."
- The new rules are designed to halt problem situations like Zubulake vs. UBS Warburg before they start.

So Now What?

- Essentially, businesses engaged in federal court proceedings are now required to have full knowledge of the whereabouts of all their electronic data to produce evidence needed in a reasonable amount of time.
- In litigation, for example, this would mean producing within 30 days relevant e-mails, text documents, spreadsheets or IMs that were originated months or years ago.
- The rules also dictate that two businesses involved in litigation must agree no later than 30 days before the first court date exactly what electronically stored evidence will be in play.

But, Let's Not Panic

- However, there is a caveat: Businesses do not have to keep everything. The rules say that documents deleted in the course of regular business are immune in the case of a litigation.
- What a business needs to show is a repeatable, predictable process of data storage and accessibility.
  - If e-mail or any other documentation is killed out of the system as a result of regular practice—such as a monthly or yearly purge of old documents—then that is acceptable to the court as being 'in the course of regular business'
  - Provided it was done prior to receiving a 'POP' Preservation Order Process.

Deploying a successful e-Discovery solution

Useful Tips

1. **Get cross-functional**: Get IT and legal departments to talk to each other as well as with records management and business line representatives.
2. **Separate backups from archives**: Mixing them makes e-discovery more difficult and expensive.
3. **Deploy ILM (information lifecycle management) methodology**: Policy-manage information with a "big buckets" approach and then move the data into more granular "little buckets."
4. **Don't boil the ocean**: Focus on efforts that provide the greatest return, such as e-mail management.
5. **Deploy search technology**: Powerful tools such as EnCase 'eDiscovery', Zantaz, Clearwell, Sherpa, can dramatically enhance e-discovery capabilities.

And Here It Is…

- SUPREME COURT APPROVES E-DISCOVERY AMENDMENTS TO FEDERAL RULES OF CIVIL PROCEDURE
  - After many years of applying the traditional paper discovery rules to electronic discovery, last week the Supreme Court approved several proposed amendments to the Federal Rules of Civil Procedure to accommodate
    - The modern practice of discovery of electronically stored information.
  - Crafted by the Committee on Rules of Practice and Procedure and approved by the Judicial Conference, the amendments are now before Congress, and will take effect on December 1, 2006.

The New Rules

- Rule 26 — General Provisions Governing Discovery; Duty of Disclosure: Subsection 26(a)(1)(B) is amended to substitute "electronically stored information" for "data compilations" as a category of the required initial disclosures. Subsection 26(b)(2)(B) is added to excuse a party from providing discovery of electronically stored information that is "not reasonably accessible because of undue burden or cost," but the burden remains on the producing party to make the required showing

The New Rules (Continued)

- Subsection 26(b)(5)(B) is added, providing a procedure for a party to maintain "a claim of privilege or of protection as trial-preparation material" concerning any discovery, even after it is produced. As the Advisory Committee Notes clarify, "Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production," but rather it "provides a procedure for addressing these issues.

The New Rules (Continued)

- new subsections 26(f)(3) and 26(f)(4) are added to make sure the Rule 26(f) conference includes a discussion of any issues relating to "disclosure or discovery of electronically stored information," and "claims of privilege or of protection as trial-preparation material." Form 35 (Report of Parties' Planning Meeting) is revised to reflect the changes to Rule 26(f).

The New Rules (Continued)

- Rule 33 — Interrogatories to Parties: Rule 33(d) is amended to specify that electronically stored information may qualify as appropriate business records from which an answer to an interrogatory may be derived or ascertained.

Zubulake v. UBS Warburg

- During 2003 and 2004, United States District Court Judge Shira A. Scheindlin issued five groundbreaking opinions in the case of *Zubulake v UBS Warburg*. *Zubulake* is generally considered the first definitive case in the United States on a wide range of electronic discovery issues.

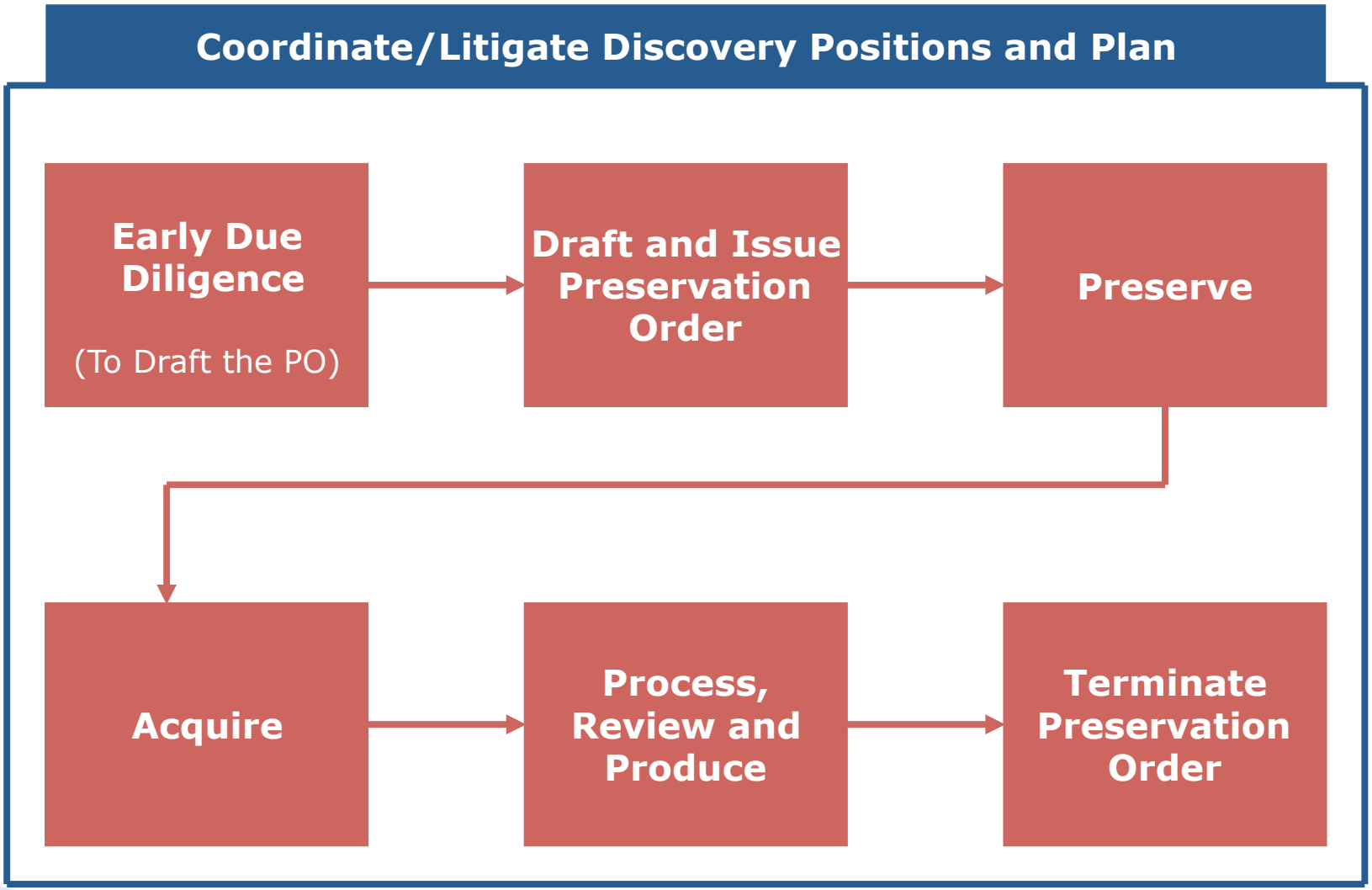
Zubulake v. UBS Warburg

(Continued)

- These issues include:
  - The scope of a party's duty to preserve electronic evidence during the course of litigation;
  - Lawyer's duty to monitor their clients' compliance with electronic data preservation and production;
  - Data sampling;
  - The ability for the disclosing party to shift the costs of restoring “inaccessible” back up tapes to the requesting party;
  - The imposition of sanctions for the spoliation (or destruction) of electronic evidence.

Methodology

Methodology

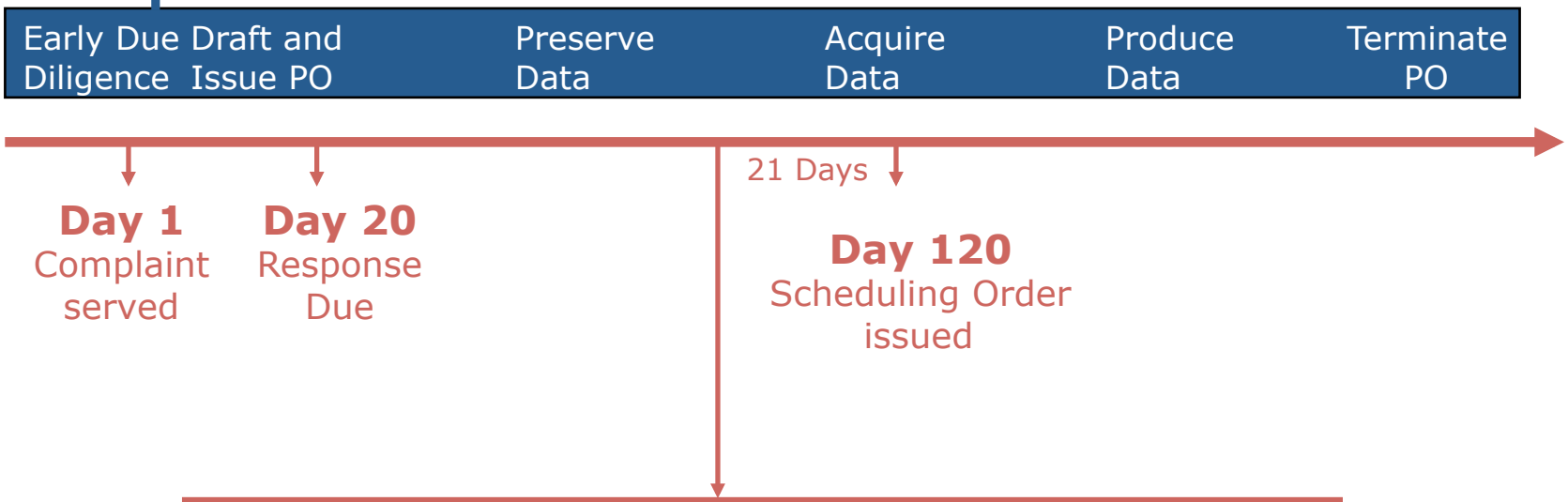


ISACA
Serving IT Governance Professionals
San Francisco Chapter

Methodology (Continued)

1. Issue a clear Preservation Order in all cases, as soon as possible
2. Issuing a Preservation Order is the beginning; manage the *entire* process
3. Coordinate Company positions in e-discovery
4. Additional tools and guidance will be issued

FRCP Amendments Early Action Required



Rule 26(f) Conference of Parties

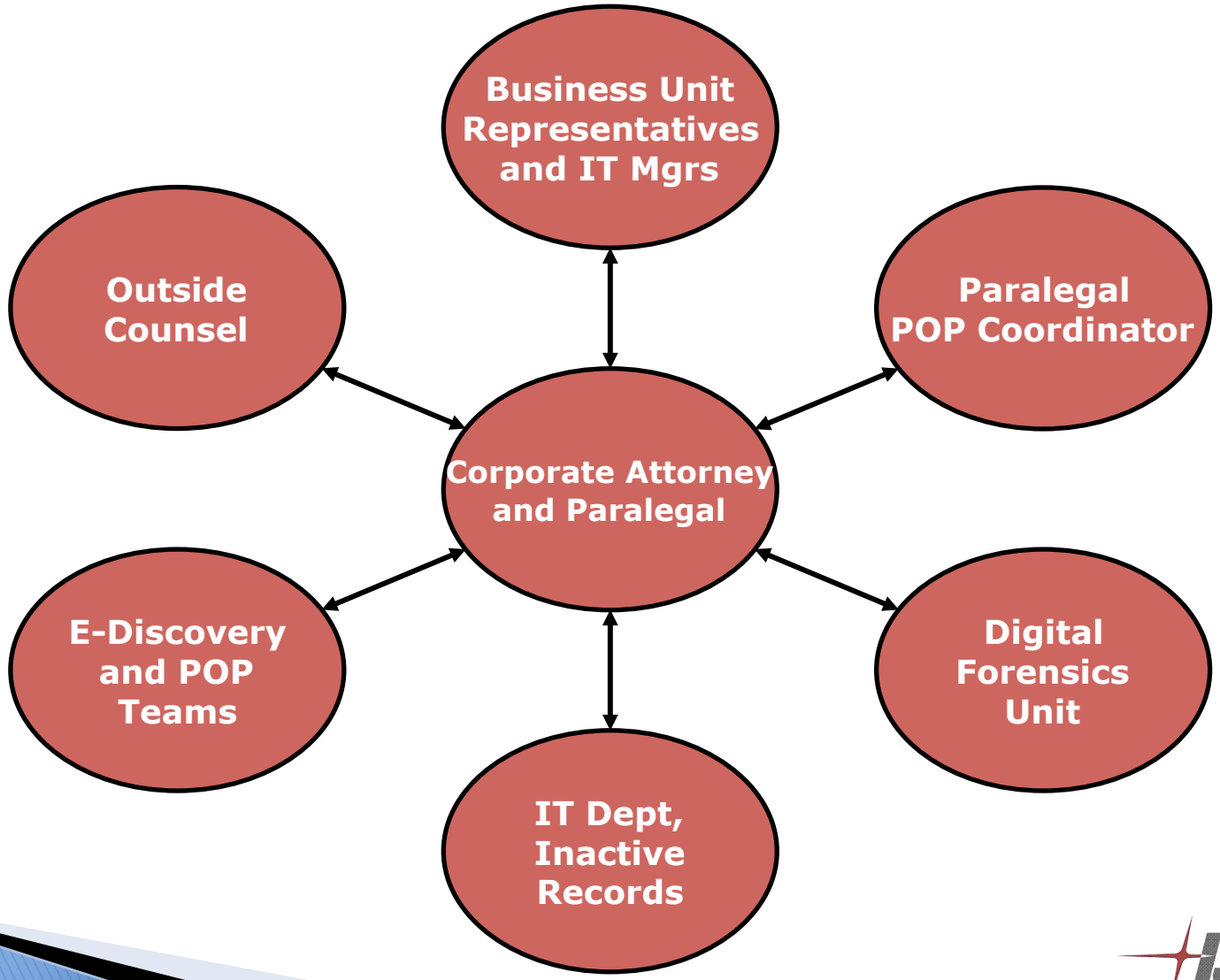
Must be able to state:

- Data searched and preserved
- Preservation efforts
- Data that is "not reasonably accessible"

Must be able to defend your actions and positions

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Early Due Diligence



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Early Due Diligence

Objectives

- Take immediate/first steps: Alert the Client
  - Duty to preserve
  - Preservation Order coming
- Get information to draft cogent Preservation Order
- Begin Planning
  - Coordinate discovery positions
  - Develop discovery plan

Early Due Diligence

Alert and Interview the Client

- **Alert client**: Duty to preserve; PO coming
- **Interview "Key Players" to draft PO**
  - What categories of information are relevant?
  - Who has relevant information?
    - How high up? BU or Corporate Executive Level?
  - What type and how much? (preview scope of discovery)
    - Hard copy: active, archived, 3rd party storage
    - Electronic data: email, Share drive, Personal drive, hard drive, what applications do you use . . .

Early Due Diligence

Begin to Identify Applications

- Alert and get help from Digital Forensics
  - **Paralegal, POP Coordinator is your point of contact for Digital Forensics.**
  - Confer with **Digital** Forensics; tell them what business functions are involved. HR, Business Units
  - **Ask Digital Forensics: what applications do these groups use?**
  - **Digital Forensics**
    - Attempting to get inventories of applications from BU's; varying degrees of completeness.
    - Close contact with IT; will identify relevant applications and IT Managers.
    - Works with Attorney to acquire data from applications.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Early Due Diligence

Begin to Coordinate Discovery Position

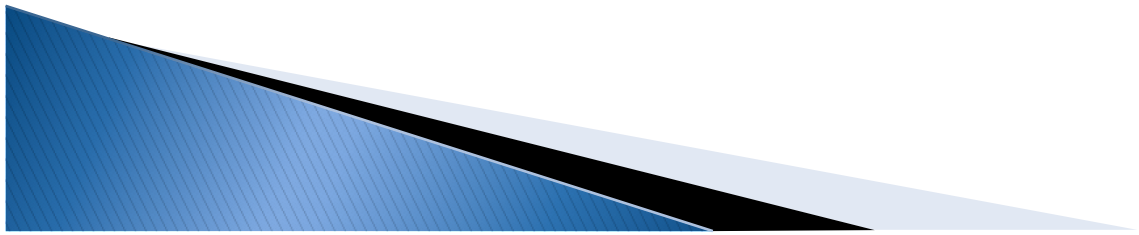
- You must take **consistent positions** on accessibility and consistently describe applications in discovery
  - Work with Digital Forensics, Outside Counsel and E-Disc. Team
  - Consider case law, interpretations of Amended FRCP, rulings on some corporations matters
- **Process for Coordinating**
  - Work with E-Disc. Team, Digital Forensics and Outside Counsel to develop position on accessibility and descriptions of applications

Early Due Diligence

Begin to Develop Discovery Plan

- **Communicate with Outside Counsel**
  - Roles of Paralegal, and Digital Forensics
  - Use processes and technology
- **Develop discovery plan**
  - Work with Outside Counsel, Digital Forensics
  - Preview potential scope of discovery
    - Volume of data
    - Nature/type of data
    - Timing and cost
- **Assess impact on Objectives, Case Plan and Budget**

Draft and Issue Preservation Order



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Draft and Issue PO

Objectives

- Issue a Preservation Order in all cases, as soon as possible
- Issue a Preservation Order that clearly states:
  - What to preserve
  - Who must act
  - What they must do
  - How to do it

Draft and Issue PO

Potential Recipients

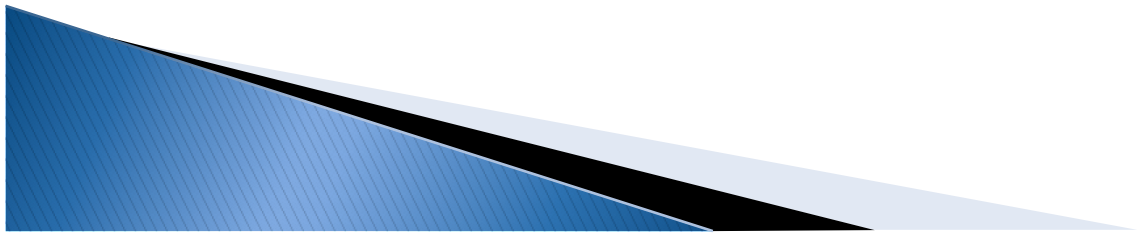
- "End User" Recipient
- IT, Inactive Records
- BU Records Custodians and Managerial Recipients
- POP Coordinator, Paralegal
  - Point of contact for Digital Forensics
  - Digital Forensics will acquire e-mail, Share-drive, Personal-drive, hard drive data.
  - Digital Forensics will identify BU applications and IT Managers, work with IT managers to acquire data.

Draft and Issue PO

Role of "End User" Recipient

- Several possible roles:
  - Recipient to create a folder, "drag and drop" relevant information; may need guidance/oversight from Attorney or Paralegal
  - Recipient to identify data location (*i.e.,* specify electronic folders in Outlook, personal drive or share drive)
  - Recipient to forward information to central repository
  - PO instructions should reflect role chosen

Preserve Data



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Preserve Data

Objectives

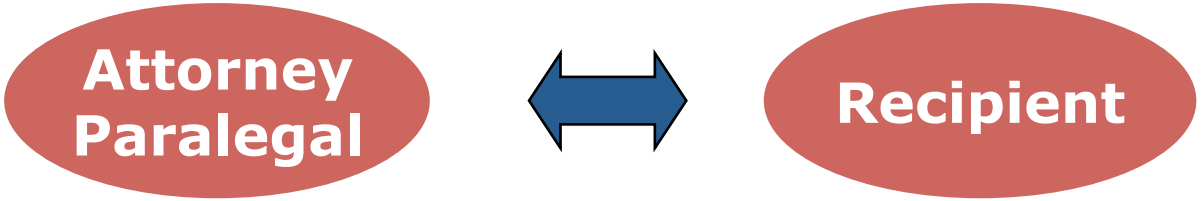
- Confirm/amend scope of Preservation Order
- Establish compliance with Preservation Order by Recipients

Preserve Data

Confirm/Amend Scope of PO

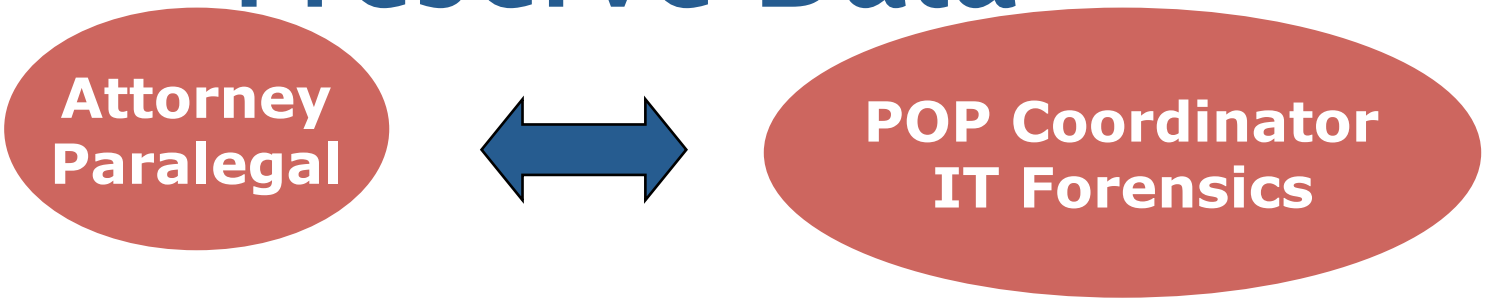
- Identify any additional *recipients*
- Identify any additional *categories of information*
- May need to supplement or amend PO as case evolves

Preserve Data



- Follow up with recipients that did not confirm compliance with PO.
  - Did you receive?
  - Have you reviewed?
  - Do you understand?

Preserve Data



- **Applications**
  - What Business Unit functions are involved in the litigation?
  - What applications do they use?
  - Which applications contain relevant data?
  - Can the application preserve relevant data? (*E.g.*, convert data to read only and cannot be deleted).
  - If not, DFG Forensics will work with IT Manager to take snapshot of data to preserve.

Rule 26(f) Conference

ISACA
Serving IT Governance Professionals
San Francisco Chapter

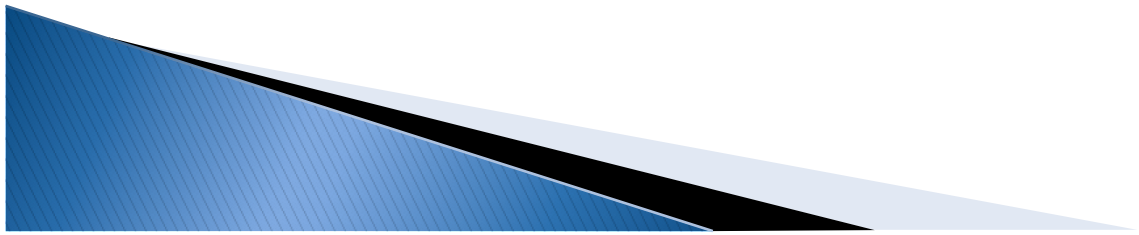
Rule 26(f) Conference of Parties

- Parties' description of:
  - data searched and preserved
  - data that is not reasonably accessible
- Parties' proposal regarding:
  - timing/sequence of discovery
  - form of production
  - privileged documents

Rule 26(f) Conference of Parties

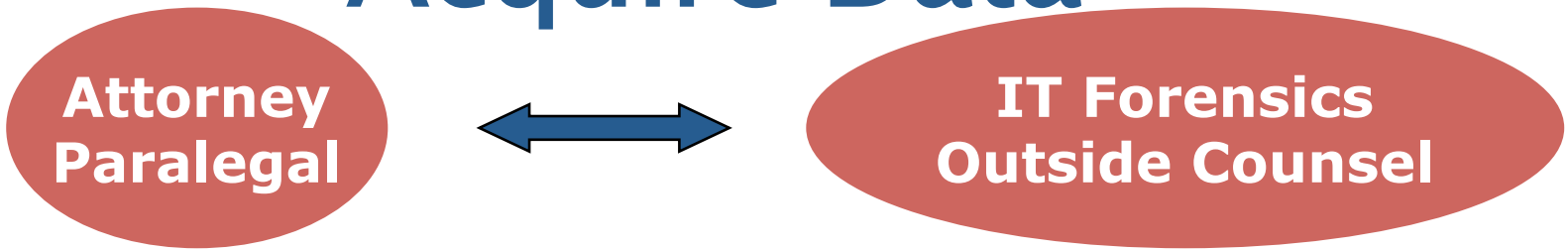
- What to expect next:
  - Motion practice on "accessibility" issue
  - Deposition of Rule 30(b)(6) Witness
  - Motion practice on timing and scope of discovery

Acquire Data



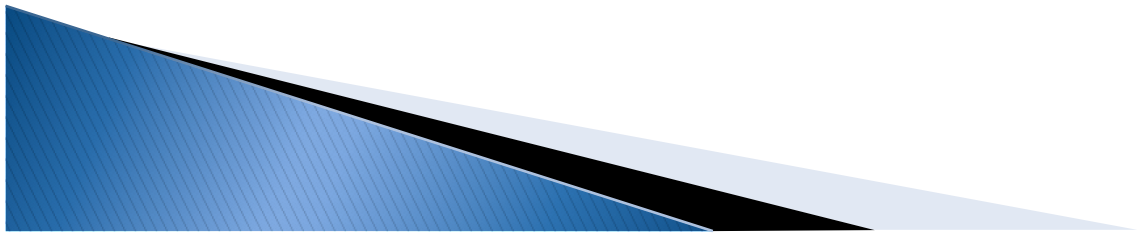
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Acquire Data



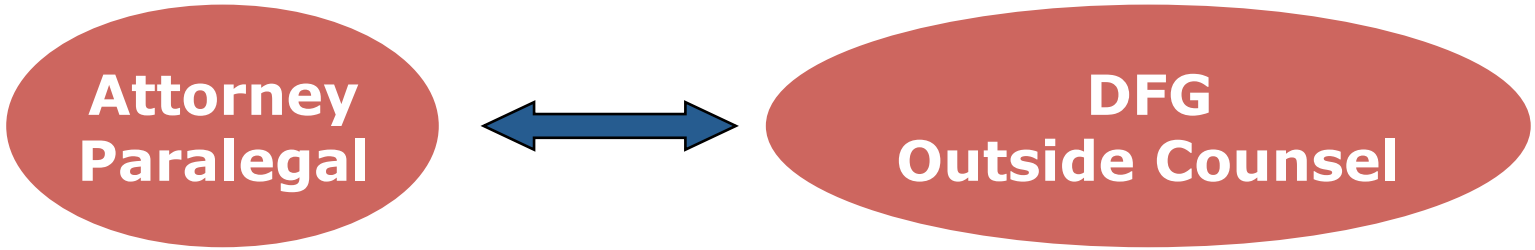
- **Execute Discovery Plan**
  - **Use Digital Forensics to acquire data**
    - Digital Forensics will acquire data identified by "End User" Recipients (*e.g.* data in e-mail, personal drive, shared drive, CD's, DVD's, thumb drives)
      - Target folders, if reasonable
      - Search terms, date parameters
    - Digital Forensics will work with Business Unit IT Managers to acquire data from applications

Process, Review And Produce Data



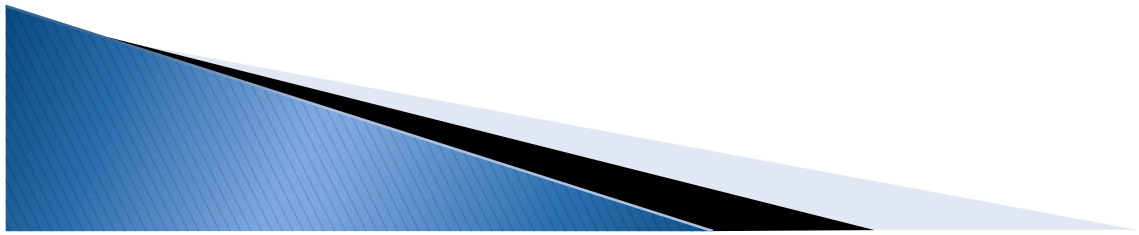
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Process, Review and Produce Data



- **Execute the Discovery Plan**
  - Roles: Paralegal and Digital Forensics
  - Corporate process and Tool used
  - Consider time required for ***all steps***: image, load, code, de-dupe, review, label and produce.

Terminate Preservation Order

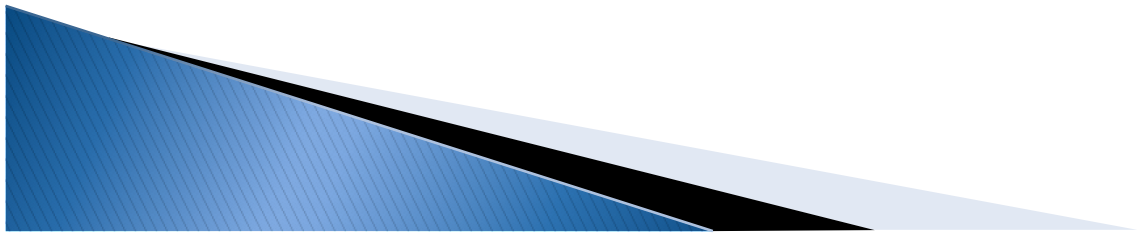


ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Objectives

- **Must** terminate PO when duty to preserve ends
- **Must** Issue Notice of Termination to all PO recipients
  - End User Recipients and IT Department, Inactive Records
    - resume management of relevant data under records retention schedule ***unless information is subject to another Preservation Order***
  - Digital Forensics: data placed on CD, send to attorney
  - Attorney: litigation file sent to offsite storage; maintain in accordance with Records Retention Schedule

The Program



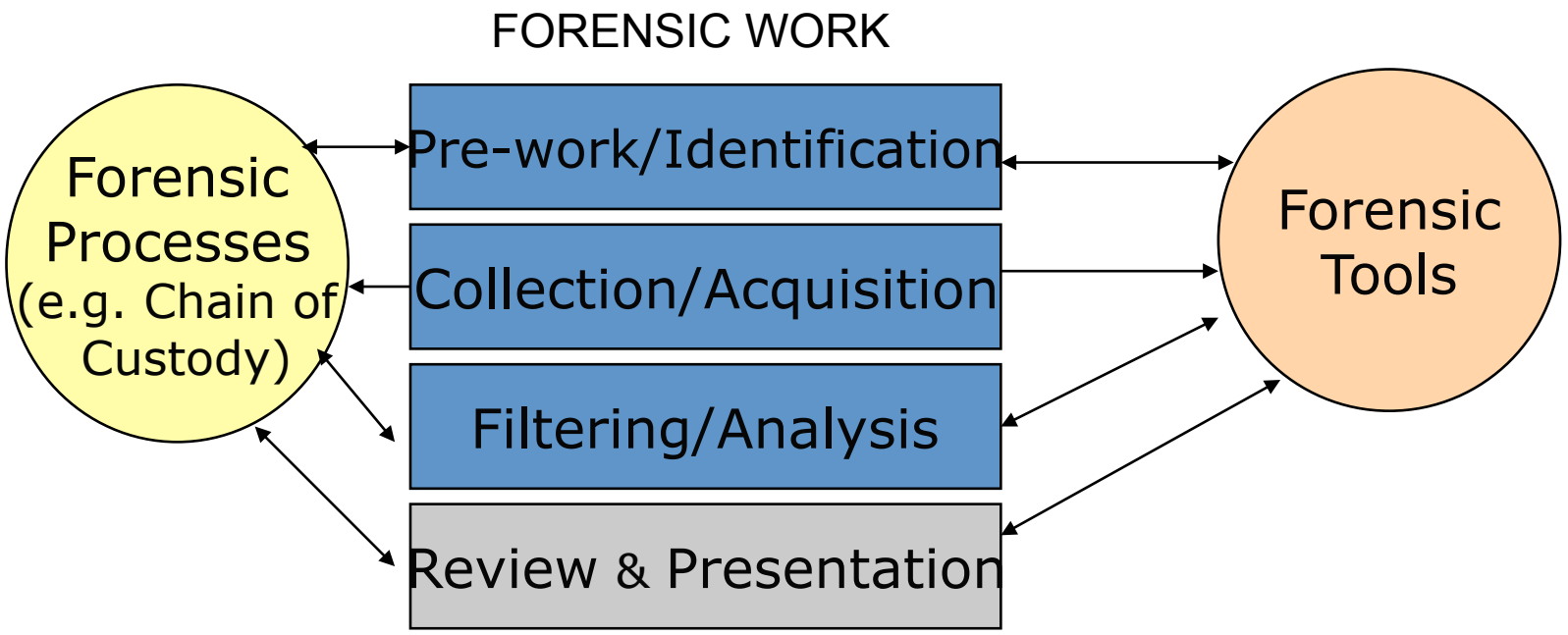
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Understanding Data Forensics

- WHAT is Data Forensics
  - A structured computer science discipline for the process of extracting information from any computer, server, database storage media and guaranteeing its accuracy and reliability
  - Carefully planned methodology that combines physical and technical investigations
  - Involves deductive reasoning, investigative skills and common sense (CSI)
- WHY does the corporation need this rigor?
  - Efficient, reliable, cost effective
  - Targeted, in-depth result of findings,
  - Evidentiary sound,
  - Centralized Expert Witness consultation and testimony

Digital Forensics Group Objective

- Build a Digital Forensic Program which is utilized for all requests of electronically stored information (ESI) (investigation, discovery, preservation, recovery, and research).



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Digital Forensics Goals

- **Don't affect Reliability.** Minimize the effect on the computer infrastructure
- **Be EFFICIENT** – Lower the cost and response time
- **Evidentiary Sound** findings. Maintain integrity of findings (prevent spoliation)
- **Accurate.** Increase the breadth and depth of ESI result
- **Maintain confidentiality** and covert process – "NEED TO KNOW" communication
- **Ethical Forensics.** Acquire **Targeted information** and Managing information appropriately…..

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Information Ethics

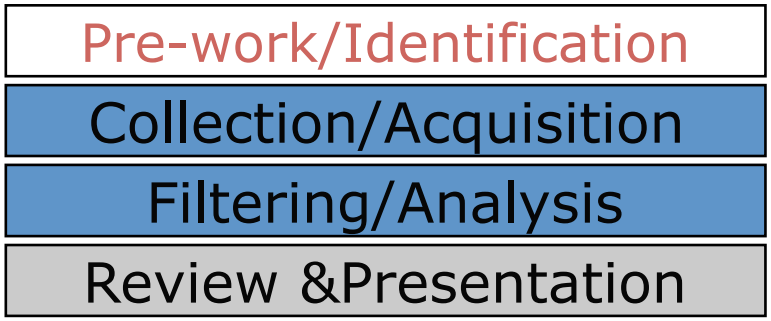
- Information from the public domain
- Private
- Legal/Privileged
- Proprietary
- Intrusive

- Awareness of the laws
- Ethical Forensics agreement, (Internal Policy)
- Background Checks
- Create Standards to limit information access to/through Digital Forensics Group (super user, hacker tools, data recovery requests…etc.)
- Governance of Digital Forensics Group (Security-Law)

Centralized and Controlled Environment for Evidence Collection

- Access to Documents stored on any Infrastructure (PCs and Servers and Network Devices)- Super authority contained to a small group.
- Data Encryption /Decryption – Keys contained to a small group
- Text Search Techniques – State-of-the-Art software
- Allowed to leverage hacker tools – DFG (Digital Forensics Group) Standard-only small group allowed to have these tools.
- Computer/Disk Search Techniques – Tools can view hidden or unused space (e.g. retrieving a previously deleted document)

Receiving Request



- Work comes through an internal process (Intranet – helps workload automation and notification)
- AUTHORITY/ENDORSEMENT: Work is submitted on behalf of managing attorney or Security must endorse request.
- Investigator calls within short period of time
- Confers with parties about case (checklist)
- DFG begin creating scope spreadsheet (what servers are involved). Create *Acquisition*, *Working* Copy, and *Findings* folders on Dedicated Forensic Server(s)

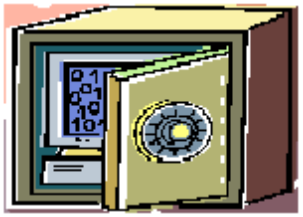
First Collection

- Pre-work/Identification
- Collection/Acquisition
- Filtering/Analysis
- Review &Presentation

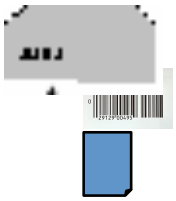
1. Locate and Prep Target Server/PC.
2. View Server and Target specific documents to acquire
3. Acquire into an “evidence file” (xxxx.L01, or xxxx.E01)

Encase Safe (Forensic Server)

Target (e.g Email Server)



5. Download a Copy of original acquisition w/hash on to a physical drive.

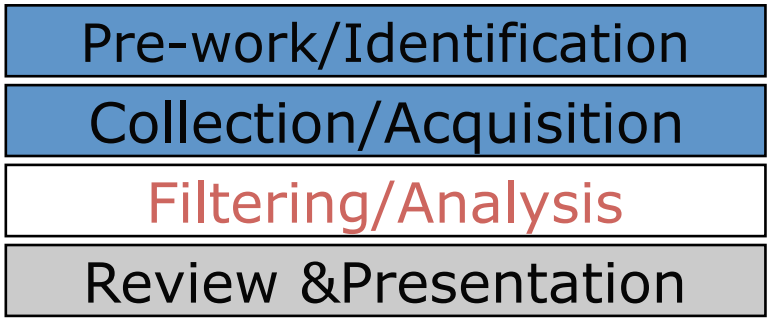


6. Barcode
7. Attach Documentation (chain of custody, drive contents)

4. Make working copy

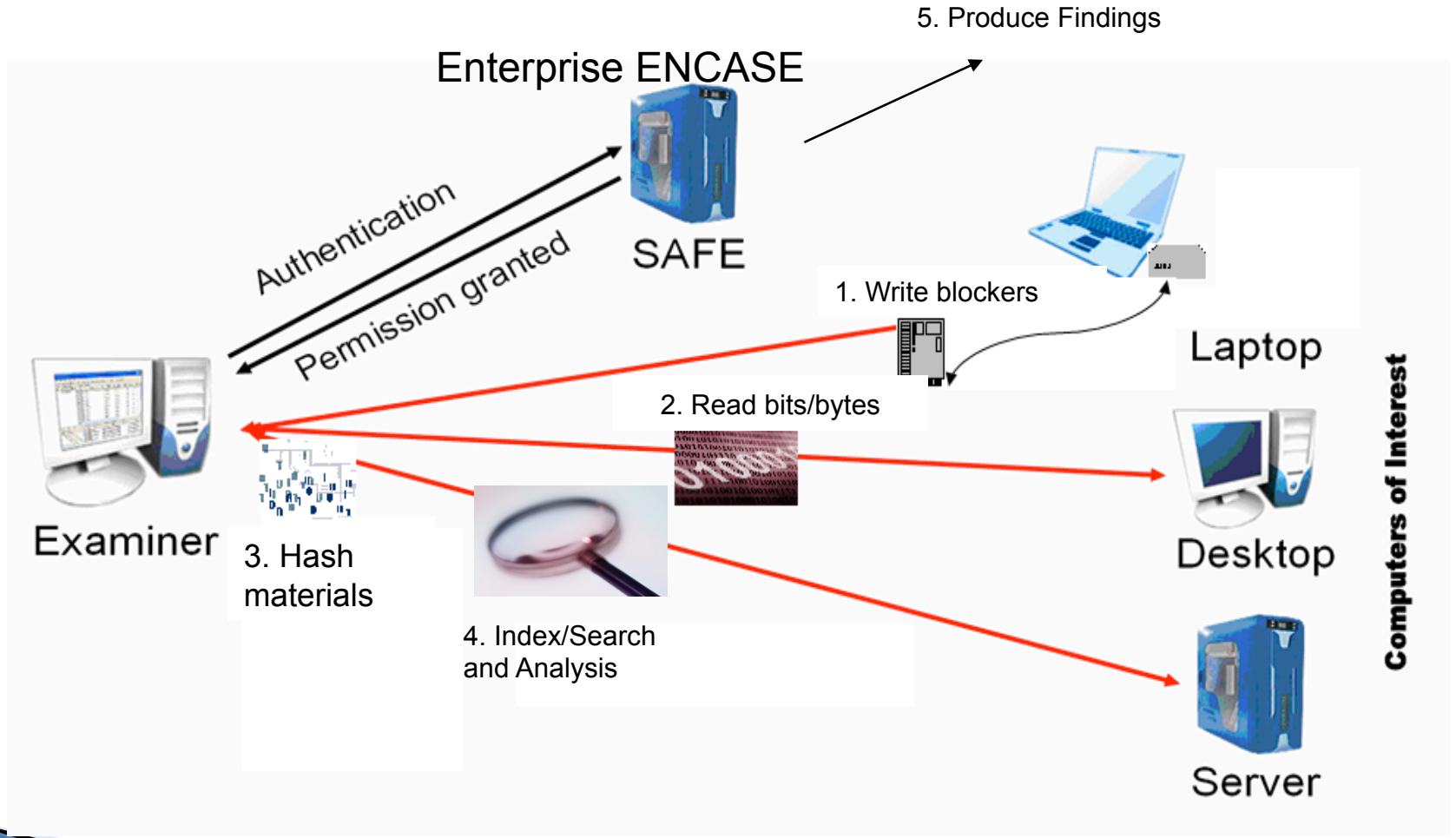
ISACA® Serving IT Governance Professionals
San Francisco Chapter

Analysis



- Using the working copy, search and analyze information understanding the case involved.
- Multiple Search tools
- Multiple iterations with attorneys
- Need to understand case and deadlines
- Target results into findings folder
- Work with Paralegal to get findings and load for review…

Forensic Process



Data Sources

- DFG should identify a series of slides which detail the various Data Sources common in corporations.
  - The Data Source slides are always evolving and should continue to be refined.
  - DFG should always be working with the legal team and eDiscovery team outside counsel, if any, on entire package.
  - The following slides include a sample Data Matrix, as well as selected supporting Data Source information.

Data Matrix

Data Type	Possible Discovery Source	Not Reasonably Accessible	Case-by-Case Determination	Under Review	Comments
MS Outlook	X				
Data on Personal Drive	X				
Data on Shared Drives	X				
Notebook/ Desktop (C:drive)	X				
Home Computer			X		Company may not have strict dominion and control, determination of accessibility will be on a case-by-case basis.
CDs/DVD/ External Drives	X				Knowledge of source is through the end -user interview process.

Data Matrix

Data Type	Possible Discovery Source	Not Reasonably Accessible	Case-by-Case Determination	Under Review	Comments
Company -owned Blackberry	X				
PDA/PIM				X	
Cell Phone			X	X	
Camera			X	X	
MP3 Player /iPod			X	X	
VoIP				X	Default business practice is not to store content. Studying the technical capability to store and the legal requirement, if any.

Data Matrix

Data Type	Possible Discovery Source	Not Reasonably Accessible	Case-by-Case Determination	Under Review	Comments
Instant Messages				X	Default business practice is not to store content. Studying the technical capability to store and the legal requirement, if any.
Voicemail				X	Default business practice is not to store content. Studying the technical capability to store and the legal requirement, if any.
Business Applications	X				
Database and Data Warehouses	X				Oracle/SQL
Collective Space Applications	X				
Video Applications or Systems	X				

Data Matrix

Data Type	Possible Discovery Source	Not Reasonably Accessible	Case-by-Case Determination	Under Review	Comments
Image Application	X				
Decommissioned and Legacy Systems			X		
Intranet Sites and Applications			X		
Intranet Sites and Static Content			X		
Backup Tape		X		X	Backup tapes are not reasonably accessible.
Printers			X		
Operational Logs and Utilities		X			

Q & A

Robert Schperberg

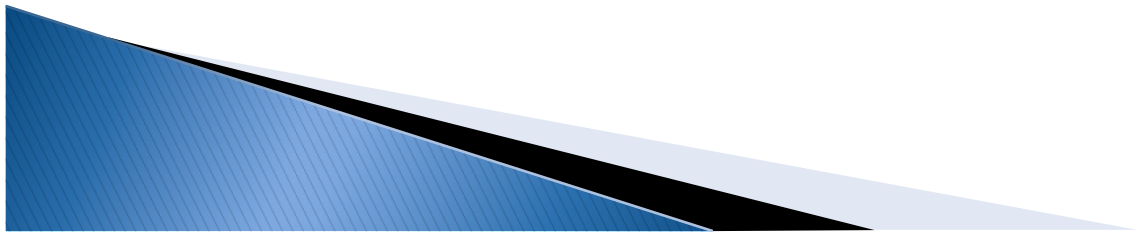
Global IT Forensics Lead

Chevron Corporation

925-842-0667 Office

209-627-7077 Mobile

rschperberg@chevron.com



ISACA®
Serving IT Governance Professionals
San Francisco Chapter