



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

January 8, 2014



# ISOAG January 2014 Agenda

- |             |                                      |   |
|-------------|--------------------------------------|---|
| <b>I.</b>   | <b>Welcome &amp; Opening Remarks</b> | <b>Mike Watson, VITA</b>  |
| <b>II.</b>  | <b>Introduction to eDiscovery</b>    | <b>Jeffery Jacobs, DTI</b>  |
| <b>III.</b> | <b>ISO Certification Program</b>     | <b>Ed Miller, VITA</b>  |
| <b>IV.</b>  | <b>CSRM Panel Discussion</b>         | <b>Benny Ambler, Bob Baskette,<br/>Jon Smith, Mike Watson, VITA</b> |
| <b>V.</b>   | <b>Upcoming Events</b>               | <b>Mike Watson, VITA</b>  |
| <b>VI.</b>  | <b>Partnership Update</b>            | <b>Bob Baskette, VITA<br/>Michael Clark, NG</b>                     |

# Introduction to Electronic Discovery



Jeffrey Jacobs, Esq.  
Associate General Counsel  
Matthew Nutaitis



© Copyright DTI  
CONFIDENTIAL Business Development Manager

# What is Electronic Discovery?

The identification, retrieval and provision (or exchange) of electronically stored information (ESI) in connection with litigation or government investigations

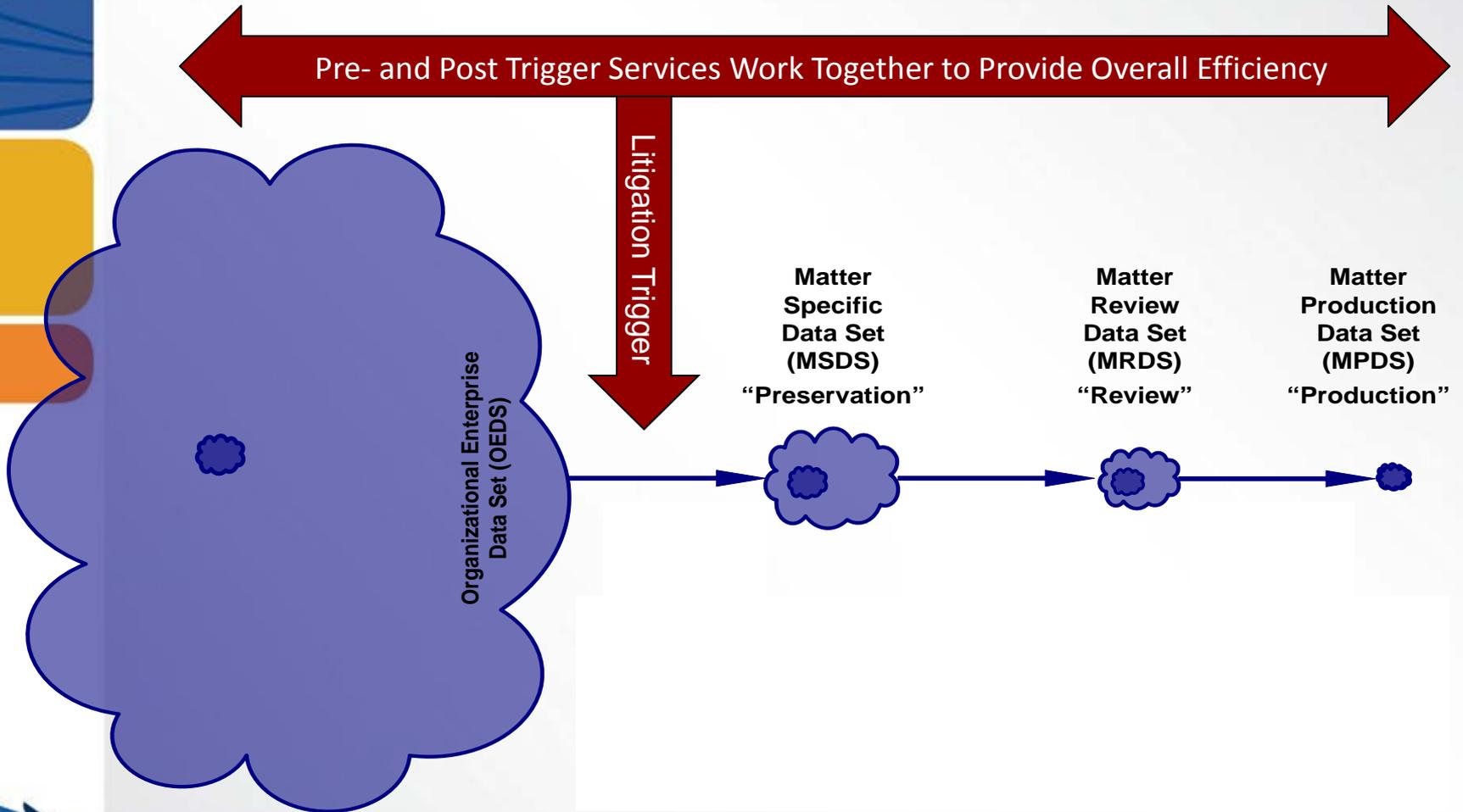


# Why Does E-Discovery Matter?

- Over 90% of all business information is never reduced to paper
- Review of electronically stored information (ESI) is the largest component of litigation expense – 70% or more
- Cases involving electronic discovery can be expensive – hundreds of thousands of dollars and more
- Electronic discovery failure, largely due to lack of litigation readiness and a response plan, can result in monetary sanctions, punitive damages, and loss of a case
- Government agencies are being held responsible for the successful conduct of electronic discovery, and need to be able to conduct it defensibly and cost-effectively



# The Discovery Challenge



# Discovery Plan

- Evaluate data landscape and universe of media of potentially relevant custodians
- Take anti-spoilation measures (litigation hold)
- Determine document review methodology (i.e., Early Case Assessment, Traditional Review, or Technology Assisted Review)
- Determine production format per the meet and confer
- Determine timelines for analysis, review and production
- Engage service provider as early as possible in this process



# Electronically Stored Information

- Otherwise known as ESI
- ESI Types:
  - Emails
    - Outlook (pst)
    - Lotus Notes (nsf)
    - Other (Groupwise, Thunderbird, AOL Mail, etc.)
  - Electronic Files and Documents
    - May include Image Files (Scanned Sets), Standard Microsoft Office Files
  - Databases, Network Applications, etc ...
    - Typically electronic files that are considered Class C or system files
  - PDAs, Smartphones, Voicemail, Video, etc.

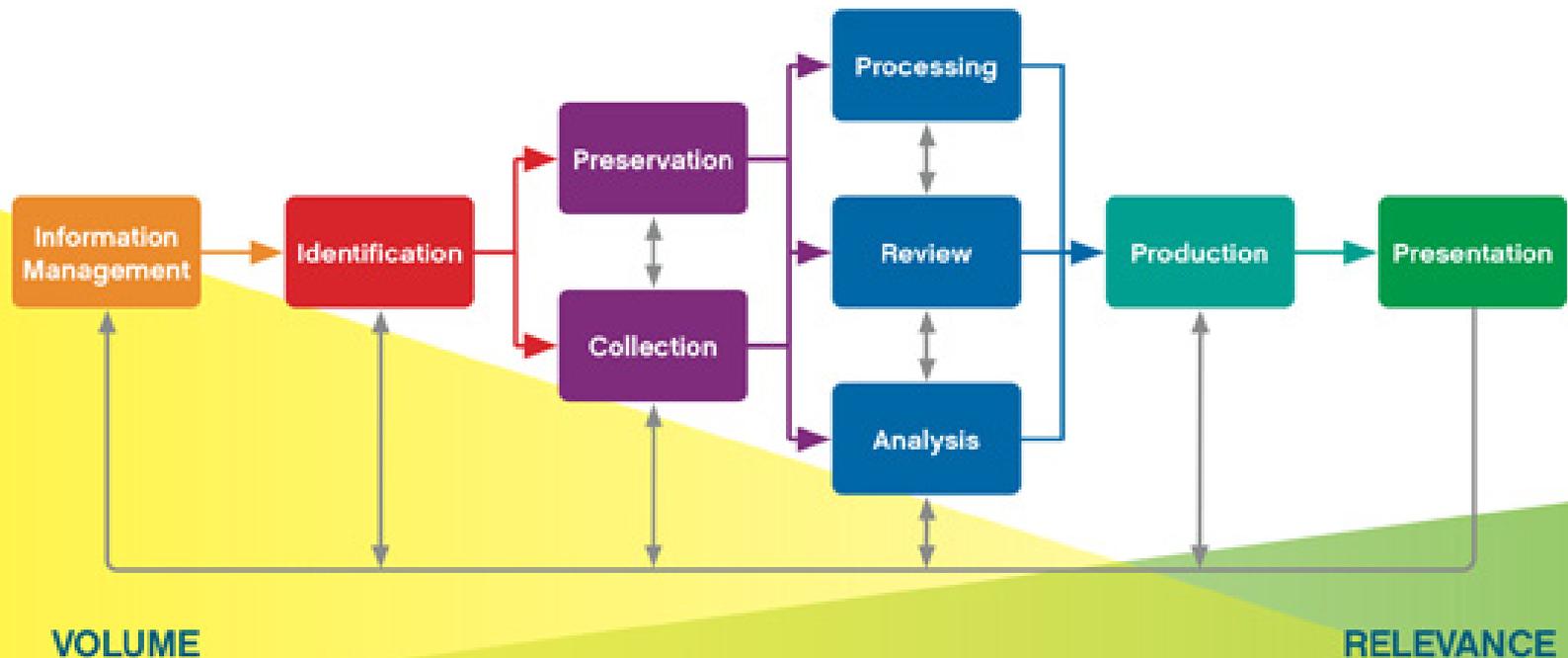
# Rule 26(f) Meet and Confer Topics

- Scope of ESI to be retrieved and reviewed
- Preservation of ESI issues (i.e., spoliation)
- Production format of ESI and other materials
- Clawback Agreement (and Order under FRE 502) to preserve privilege in face of inadvertent production
- Shifting costs from Producing Party to Requesting Party



# The Electronic Discovery Reference Model (EDRM)

## Electronic Discovery Reference Model



Electronic Discovery Reference Model / © 2009 / v2.0 / edrm.net



# Identification

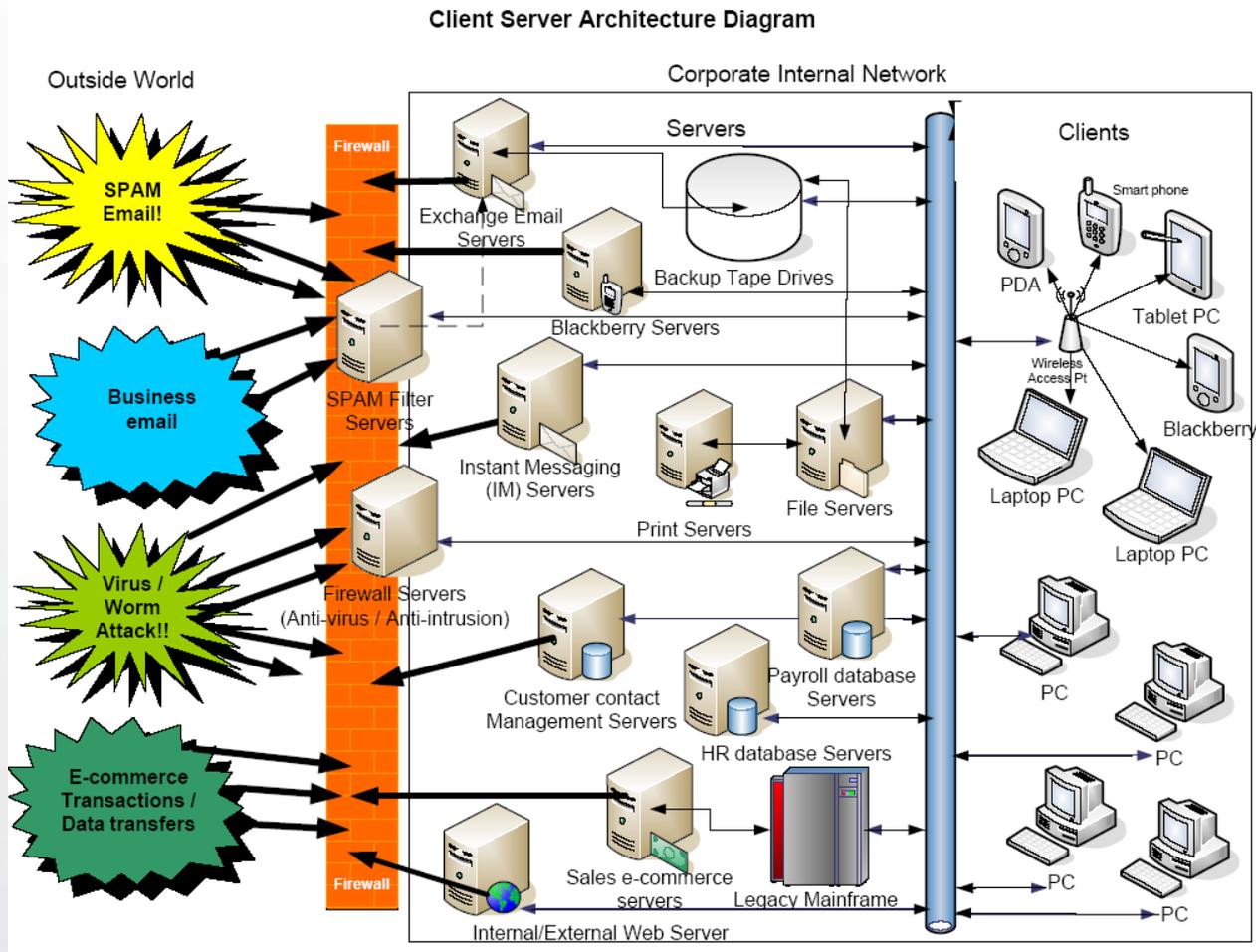
- This phase of the EDRM is to identify the sources and locations of the pertinent information for the matter.



Although represented as a linear workflow, moving from left to right, this process is often iterative. The feedback loops have been omitted from the diagram for graphic simplicity.

# Architecture Diagram

## Know where your data is at all times!



# Preservation

- To ensure you meet all the requirements set forth for the matter, you'll want to implement a preservation plan for all potentially relevant data.

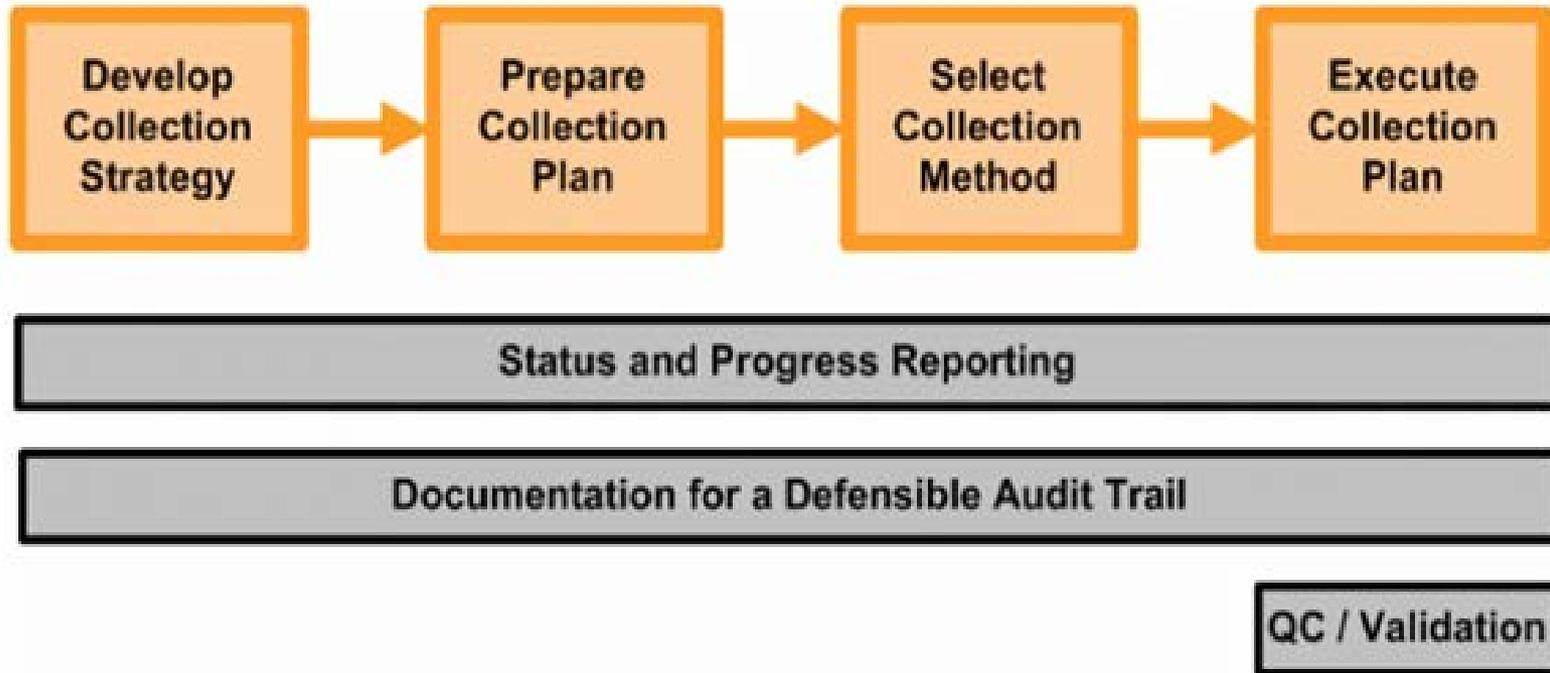


# Preservation Best Practices

- Cease routine destruction (through IT and Records Management) and issue written hold notices to potential custodians once litigation is “reasonably anticipated”
- May need to preserve before litigation is filed or complaint/subpoena is received
- Confirm acknowledgment and understanding of hold obligations by custodians
- Watch out for data of departed, departing or transferring employees
- Issue periodic hold reminders
- Lift hold when matter ends, ensuring that multiple hold custodians are aware of ongoing obligations
- **DOCUMENT EVERY STEP**



# Collection

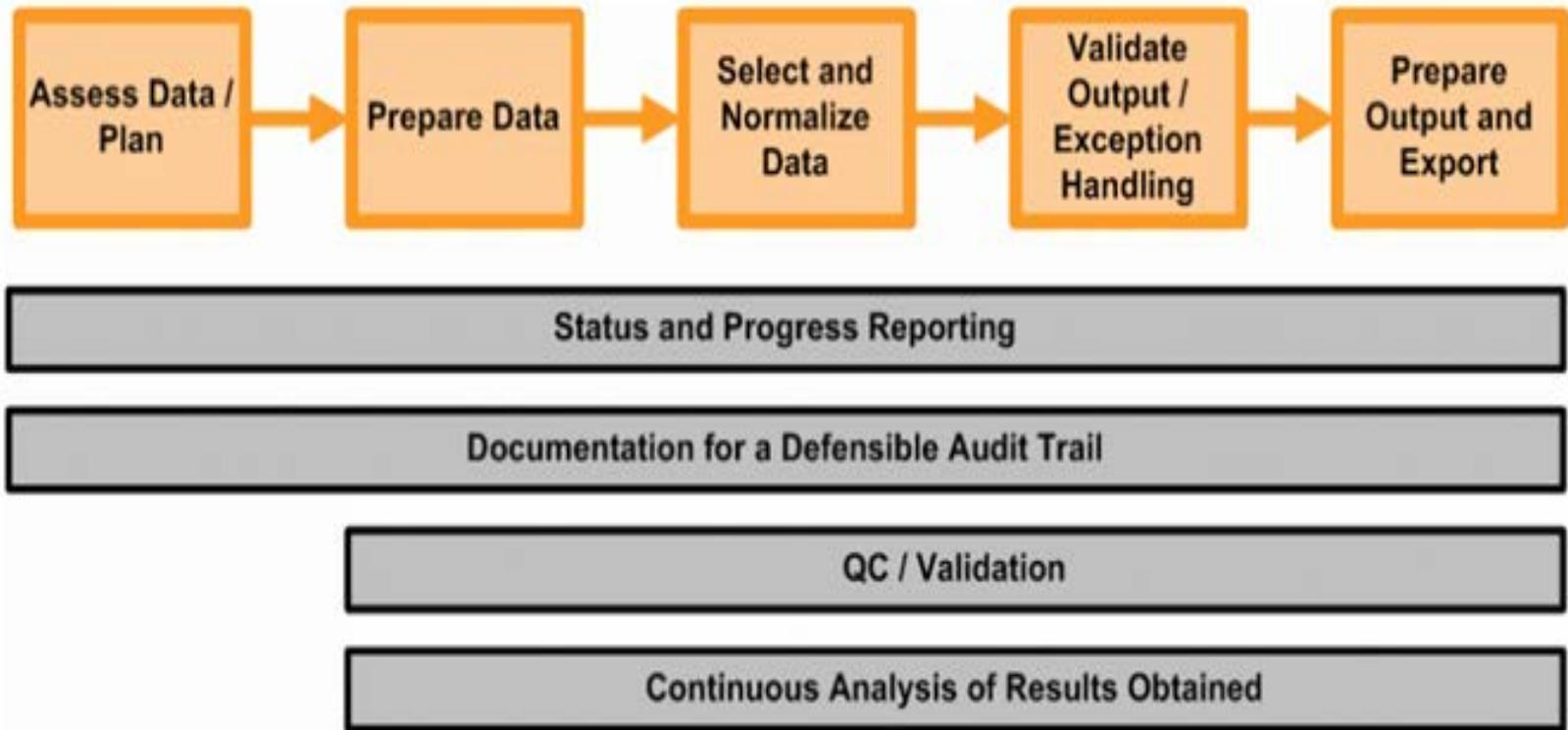


# Collection Best Practices

- Once data has been identified and preserved it is now time to determine the collection method
- Make sure you maintain chain of custody through the collection phase and record the recovery procedures
- Early Organization – as soon as you know that data will need to be collected
- Schedule Custodians prior to collection technician's arrival – allows for an easier and more efficient data collection
- Distribute custodian questionnaires prior to collection to determine system types, data volumes, custodial history, passwords
- Determine whether collection will be targeted, forensically sound (logical) or full forensic image captures for custodians and server environment



# Processing

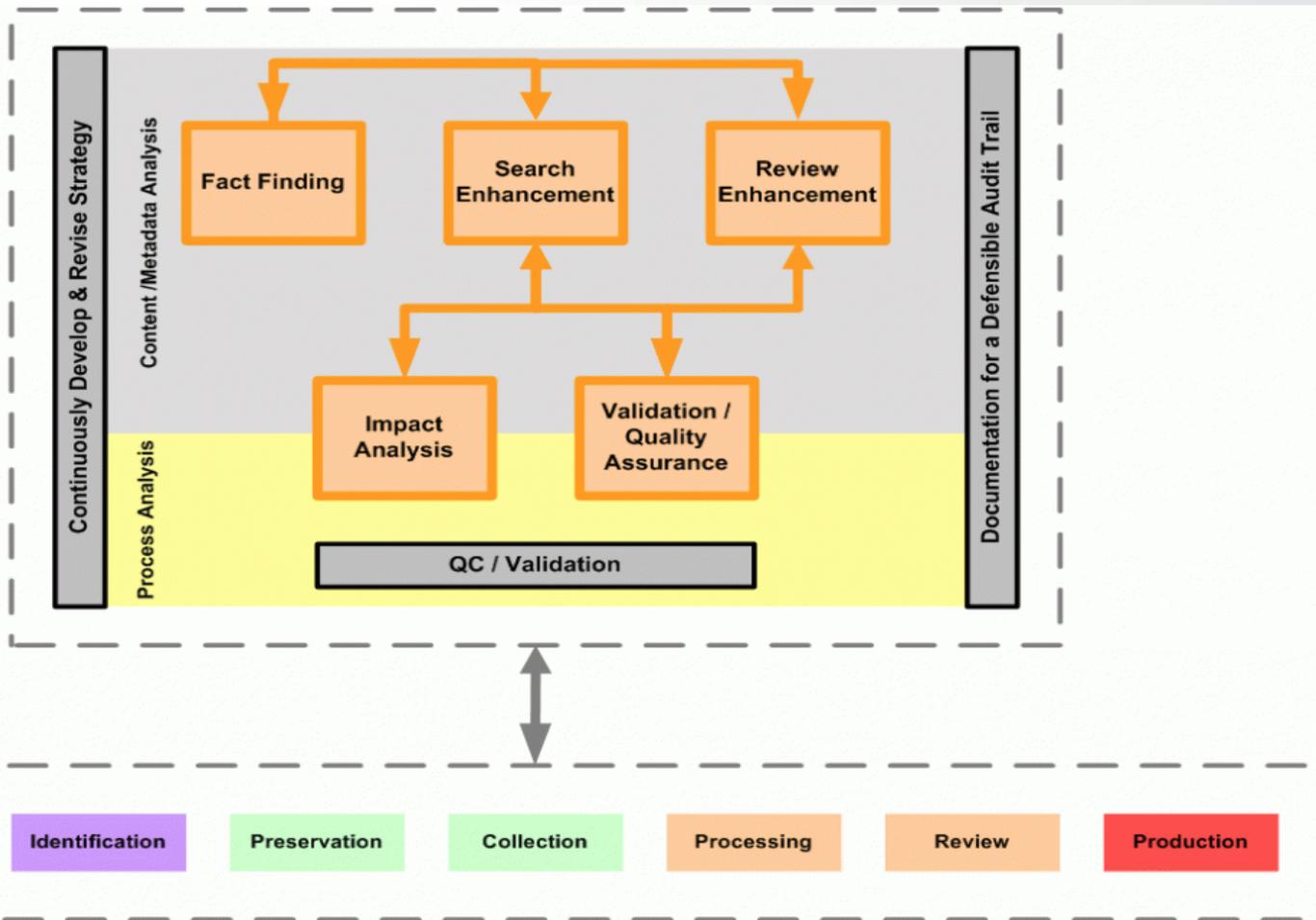


# Processing Best Practices

- Prioritize custodians – most important custodians first
- Before proceeding with processing, determine whether analysis is needed, which can depend on the amount of data and how it was collected
- Now that you're ready for processing you'll need to determine your culling/filtering techniques (i.e., de-duplication, de-NIST, search terms, date restrictions, specific custodians or file types, etc.)
- Custodian De-Duplication method (within custodian or across entire data population)
- TIFF or PDF files – if no searchable text is present, you should use Optical Character Recognition (OCR) to make them searchable



# Analysis

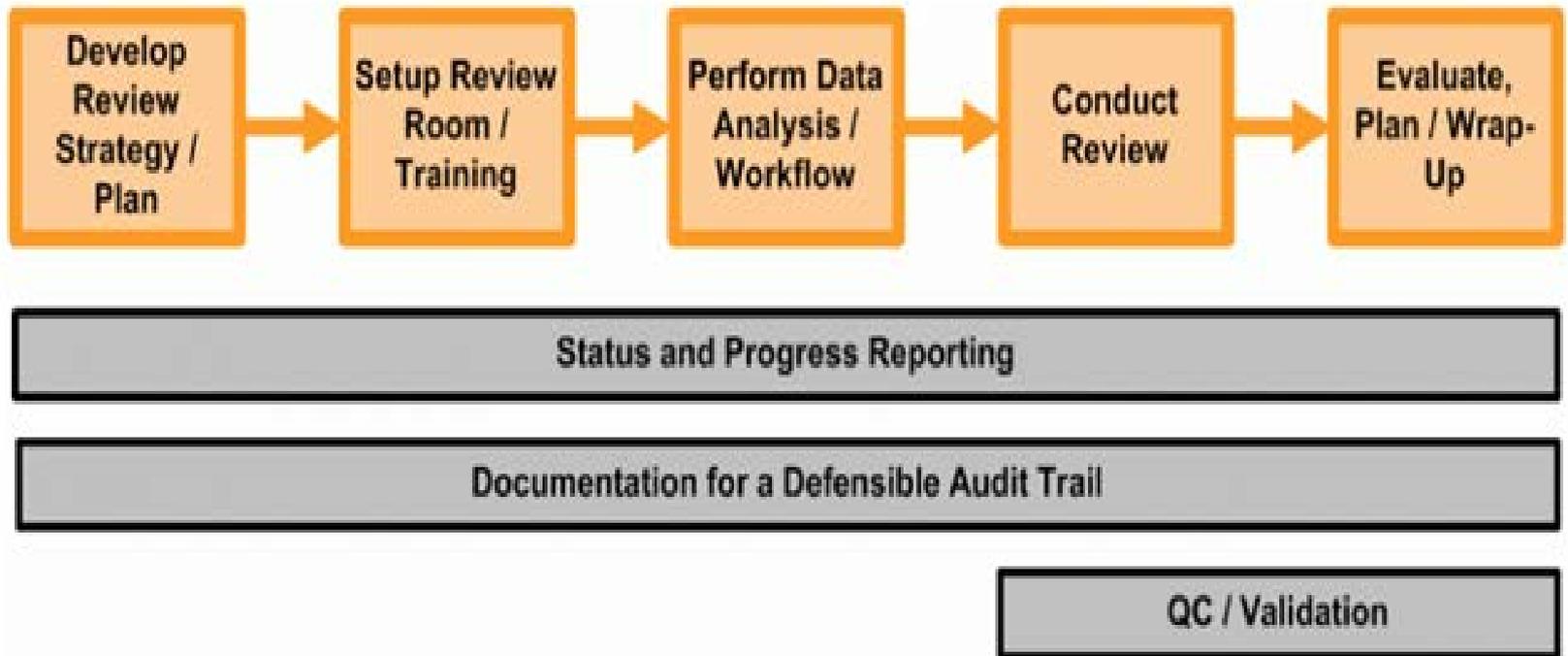


# Analysis Best Practices

- Determine if the matter calls for an Early Case Analysis using consultants and appropriate technology
- If uncertain about key words and culling strategy, use a consultant to help analyze the case and what potential words/phrases could assist with expanding the key word list
- Aspects of analysis can still occur during review to help provide a streamlined and cost-effective outcome, and also as a QC measure



# Review



# Review Best Practices

- If detailed analysis wasn't done prior to data migration into review, need to decide what, if any, analysis should be done (conceptual analysis, email thread identification, near-duplicate analysis, etc.)
- Review is a collaborative effort between the client, outside counsel and service provider to ensure an efficient review workflow
- Define data review stages (1st pass, 2nd pass, privilege review)
- Develop standard review fields/tagging pane and associated special tags that corresponds to each
- Determine how many reviewers will be assigned during each phase of review, in order to meet internal and mandatory deadlines
- Highlight relevance-related and potentially privileged search terms (including attorney names/firm domains) to speed review
- Utilize the reports that are available to track review progress
- Fully understand and take advantage of review platform features
- Consider contract (including offshore) review and Technology Assisted Review



# Production



Status and Progress Reporting

Documentation for a Defensible Audit Trail

QC / Validation



# Production Best Practices

- Pre-planning is key - production format and specifications should be determined early and agreed upon with opposing counsel
- Know TIFF formatting specs
- Due to cost considerations, try to avoid tiffing spreadsheets; produce natively when possible. Of course, some matters may require full TIFF productions.
- Establish a special tag to identify documents to be produced - easier to quality control the export
- Quality control production prior to delivering to a 3rd party such as opposing counsel or government entity
- Ensure privileged documents are slip sheeted and that there are not any privileged parents without privileged attachments and vice versa
- Allow yourself enough time to produce in a timely manner, with adequate QC!!



# Discovery Sanctions in 2012

- Sanctions granted in 69 federal cases
- Monetary sanctions up to \$1 million in 44 cases
- Adverse inference instructions in 20 cases, including one where a defendant destroyed his computer with a sledgehammer
- Evidence excluded in 10 cases
- Termination orders in 5 cases



# Significant eDiscovery Cases

- Zubulake (2004) -- \$29.3 Million Verdict
  - \$9.1 Million Compensatory
  - \$20.2 Million Punitive
- Morgan Stanley (2005) – \$1.45 Billion Verdict
  - \$600 Million Compensatory
  - \$850 Million Punitive
  - \$20 million demand before trial

(Reversed on unrelated, technical grounds)
- Qualcomm (2007) -- \$8.5 million attorneys fee award
- National Day Laborer v. USICE (2011) – Metadata part of Federal records and required for FOIA production

# ***Zubulake v. UBS (2003 - 2005)***

- Sanctions: Adverse inference instruction & costs
- \$29.3 Million Verdict
  - \$9.1 Million Compensatory
  - \$20.2 Million Punitive
- Legal hold alone is not enough → Counsel failed:
  - To communicate with key players
  - To monitor compliance
  - To locate relevant information

# The Zubulake V Opinion

- Counsel must:
  - Actively monitor compliance with litigation hold
  - Become fully familiar with client's document retention policies, data retention architecture and electronic systems, and communicate with all key players regarding their ESI storage and retention obligations
  - Ensure that backup tapes or other backup media are retained if they are the only source of potentially relevant information

## For further information:

Jeffrey Jacobs, Esq.  
Associate General Counsel  
[Jeff.Jacobs@dtiglobal.com](mailto:Jeff.Jacobs@dtiglobal.com)  
(202) 361-9887

Matthew Nutaitis, Jr.  
Business Development Manager  
[MNutaitis@dtiglobal.com](mailto:MNutaitis@dtiglobal.com)  
(202) 842-3300





Virginia Information Technologies Agency

# Commonwealth ISO Certification Program Continuing Education Requirements

Ed Miller  
Security Analyst, VITA

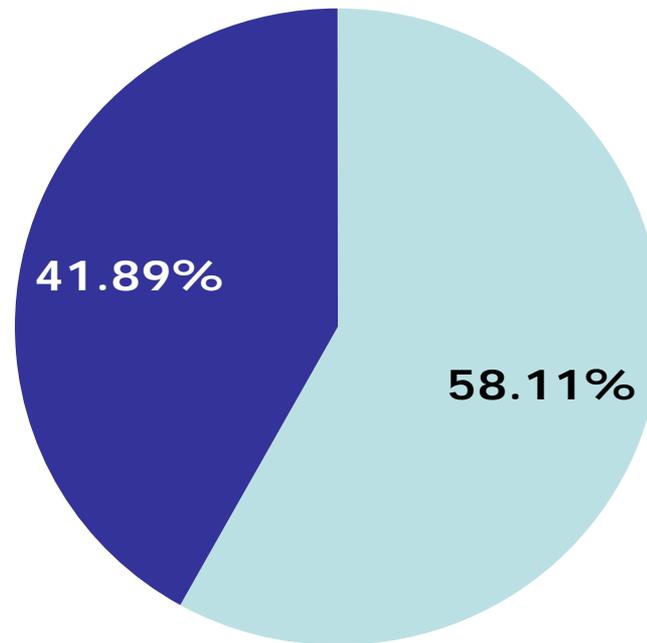


# Commonwealth ISO Certifications 2013

## Commonwealth ISO Certifications 2013

Commonwealth Certified ISOs'  
58.11 %

Non COV Certified ISOs'  
41.89%





# Maintaining Your Certification

In order to maintain your status as a Commonwealth Certified ISO in 2014, you need to meet 4 basic conditions:

1. Agree to the Commonwealth IT Security Code of Ethics
2. Attend any mandatory ISOAG meetings in 2014
3. Attend IS Orientation once every 2 years
4. Obtain 20 hours of continuing education credit per year



# 1. Code of Ethics

ISOs' are entrusted with an agency's most highly confidential and sensitive information.

Ethical behavior, both on and off-the-job, is the assurance that COV ISOs' are worthy of that trust.



## Commonwealth IT Security Code of Ethics

- Perform all professional activities and duties in accordance with all applicable laws, commonwealth regulations and the highest ethical principles
- Promote current and generally accepted information security best practices and standards
- Maintain appropriate confidentiality of sensitive information encountered in the course of professional activities
- Discharge professional responsibilities with diligence and honesty
- Refrain from any activities which might constitute, or give the appearance of, a conflict of interest or otherwise damage the reputation of the agency or the COV



## 2. Mandatory ISOAG Meetings

- Once again, we will have a mandatory meeting of all ISOs' in October.
- We encourage all primary ISOs' to attend this meeting in person.
- If you are a primary ISO, and cannot attend, you may designate the backup ISO to attend in your place.



## 3. Attend IS Orientation Every 2 Years

- All ***primary ISOs' are required*** to attend this 2 hour session at least once every 2 years. The requirement to attend cannot be delegated to a backup ISO or other person unless approved by the CISO. However, backup ISO's and other interested persons are encouraged to attend.
- We are continually changing and evolving the content provided in the IS Orientation session. Some sessions will be offered that will look closer at specific ISO learning areas: Risk Assessments, Policies, Control Implementation, Security Plans, etc.



## 4. Continuing Education Requirements

- In order to maintain the COV ISO Certification, ISOs' must commit to furthering their education.
- The goal is to ensure that all ISOs' are maintaining a minimal level of current knowledge and proficiency in the field of Information Security.
- In 2014, the continuing education requirement will be 20 hours. Each hour of conditioning education is known as a CPE (continuing professional education) credit. CPE can be obtained in a number of ways.



## Continuing Education Requirements

- At least one of the 20 CPE credits, must be obtained by completing 1 course in ISO Academy in the Knowledge Center. For the purposes of this requirement, we will equate 1 ISO Academy course to 1 hour or credit of continuing education.
- We will be adding additional (new) courses to Knowledge Center in 2014.



## Continuing Education Requirements

- If you already have a nationally recognized IT security certification, then any continuing education that is required by that certifying authority will also be honored by the COV Certification program.
- You **do not** need to obtain an additional 19 CPE hours above and beyond what you are already reporting for continuing education for any other nationally recognized IT security certifications. In other words, the 19 hours that you acquire for your CISSP, CISM, GIAC or other recognized certification can also be applied to your COV ISO Certification.



## How to Earn Continuing Education (CPE)

- Take add'l IT security courses in the KC ISO Academy (1 course=1 hr)
- Attend training courses or seminars related to IT Security
- Attend IT security conferences
- Attend ISOAG Meetings
- Attend chapter meetings of a recognized IT security organization
- Take IT security related academic courses at a higher ed institution
- Complete IT Security related webcasts, podcasts or other computer based training
- Read IT security related books or articles (limit of 10 hrs/year)
- Publish an IT Security related book or article
- Attend vendor sales/marketing presentations (limit of 5 hrs/year)
- Teach or present on an IT security related topic
- Serve or volunteer for committee work on the **COV Security Council**



# Calculating Continuing Education (CPE)

- In general, one continuing education hour will be earned for 50 minutes of active participation in the activity (excluding breaks).
- Divide the total # of minutes in the activity less time for breaks by 50 rounded to the nearest 15 minute increment.
- For example:

Activity	# hours	# of minutes
IT security seminar: 9 am to 5 pm	8.0	480
LESS: 2 15 minute breaks	0.5	30
LESS: 1 hour for lunch	1.0	60
TOTAL: of qualifying activity	6.5	390
390 minutes / 50 =	7.8	
Round to nearest 15 minute increment	7.75	CPE



## Calculating Continuing Education

- Reading an IT security related book or article should be calculated as 50 pages equaling 1 hour.
- For some activities, you may receive a “certificate” from the sponsoring organization that indicates the # of CPE credits earned. In that case, you do not need to calculate the # of hours, we will accept the calculation of the sponsoring organization (keep the certificate for your records).
- Additional hours, above & beyond the minimum of 20 required, are strongly encouraged but cannot be rolled-over and applied in subsequent years. The 20 hours you are claiming must be earned in the calendar year being reported.



## Reporting Continuing Education to CSRSM

- When you have completed ***all 20 hours*** of required continuing education activities in 2014, send an email to [commonwealthsecurity@vita.virginia.gov](mailto:commonwealthsecurity@vita.virginia.gov) indicating that you have completed. We do not need notification for each time you complete a specific or individual activity.
- Please include in the email a brief description of the activities that you have completed.



# Maintaining Continuing Education Records

- Maintain for your own records, any documentation that indicates you have completed the activity. Include in your documentation, the name of the activity, the date, time, and hours claimed. You should also keep for your records, any certificates of completion, receipts, program outlines, agendas, brochures, handouts, etc. for any activity that you complete.
- You should maintain your own records of your participation in the activity for 3 years.
- You **do not** need to send any of this documentation to CSR, but it is possible, in some cases, that we or an auditor may ask or need to see it, so please maintain a personal file of this information.



## Summary of Continuing Education Req's.

1. Agree to abide by the Commonwealth IT Security **Code of Ethics**
2. Attend any **mandatory ISOAG meetings** in the coming year
3. Attend **IS Orientation** at least once every 2 years
4. Obtain **20 hours of continuing education** in IT Security per year



# Questions on Continuing Education?



**Ed Miller**

**VITA**

**Commonwealth Security & Risk Management**

**804-416-6027**

**[edward.miller@vita.virginia.gov](mailto:edward.miller@vita.virginia.gov)**



Virginia Information Technologies Agency

# CSRM Panel Discussion

Benny Ambler, Sr Mgr Security Governance

Bob Baskette, Sr Mgr Security Operations & Architecture

Jonathan Smith, Sr. Mgr Risk Management

Michael Watson, Chief Information Security Officer



Virginia Information Technologies Agency

# Upcoming Events





## CIS/MS-ISAC & SANS

### *Center for Internet Security & SANS Institute for Security Awareness Training*

As part of the Center for Internet Security and SANS partnership agreement they are offering this aggregate purchasing opportunity for state, local, territory and tribal governments, as well as related educational and not-for-profit entities, during the ***December 1, 2013 to January 31, 2014*** timeframe.

***Please follow your agencies procurement policies and procedures when purchasing security training***

For more information:

<http://alliance.cisecurity.org/opportunity/training.cfm>



## Upcoming Training

### *Public Speaking for Auditors*

Date: January 29 & 30, 2014

Time: 8:15-4:45

Location: TBD

Cost: \$ 320.00

### *IT for non-IT Auditors*

Date: February 5

Time: 8:15-4:45

Location: TBD

Cost: \$160.00

**Register:** <https://hrtraining.doa.virginia.gov>



# Future ISOAG

**Feb 5            1:00 – 4:00 pm @ CESC**

**Keynote: “Incident Management”**

**with Karen McDowell, UVA**

***ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2014***



# IS Orientation

**When: Thursday, March 6, 2013**

**Time: 9:00 am to 11:00 am**

**Where: CESC , Room 1211**

**Register here:**

**<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>**

**Next IS Orientation will be held on Jun 5, 2014**



## Save The Date

### **IT Security Conference** ***“Information Security Enabling the Business”***

**Date: April 3 & 4, 2014**

The event will include numerous topics.

*More details will be provided soon!*



## Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# ISOAG-Partnership Update

*IT Infrastructure Partnership Team  
Bob Baskette*

8 January, 2014



**NORTHROP GRUMMAN**



# ADJOURN

## THANK YOU FOR ATTENDING

