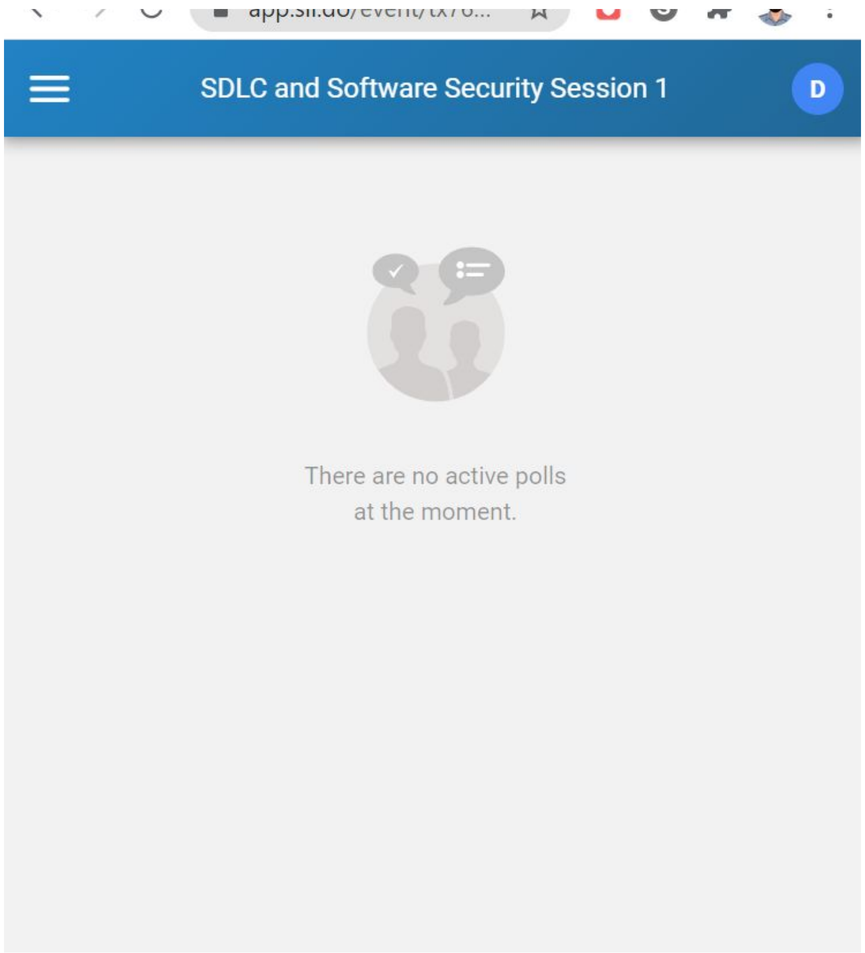


SDLC and Software Security Session 1

There are no active polls at the moment.

While we wait…

Please check if you can open the Quiz.
Go to the URL

https://icsbits.com/go/cisspjam

Quiz will be available at the end of this session

General Discussion Forensics for CISSP.

Terms and Concepts.

Domain 7: Security Operations Session 1

By DK

<u>60- 90 min</u>

Hello!

Notes:

Pinned Messages on Classroom-1

www.icsbits.com/go/notes

Today's Discussion

- Investigation Types
  Terms and Concepts - Burden of Proof, Computer Forensics, E-Discovery
- Evidence and Types
- ISC2 Code of Ethics
- Quiz Time!

Types of Rules and Types of Investigations.

Criminal Law	Criminal Investigation
Civil Law	Civil Investigation
Administrative Law	Agency Investigations
Private Regulations	Private Investigators
Company Policies	Administrative Investigation

Table 1

Types of Investigations Contd..

Criminal Law	→ Break → Criminal Investigation→ Arrested and Jail
Civil Law	→ Break → Civil Investigation → Fined
Administrative Law	→ Break → Agency Investigation → Criminal/Civil→ *
Private Regulations	→ Break → Private Investigators → Criminal/Civil→ *
Company Policies	→ Break → Internal HR investigation → Fired / Criminal/Civil →

Burden of Proof ---> Beyond Reasonable Doubt

Civil Cases

Documentation and Proof

Criminal Cases

Witness, Documentation, Experts

Computer Forensics

is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. -*Techtarget*

Some more terms

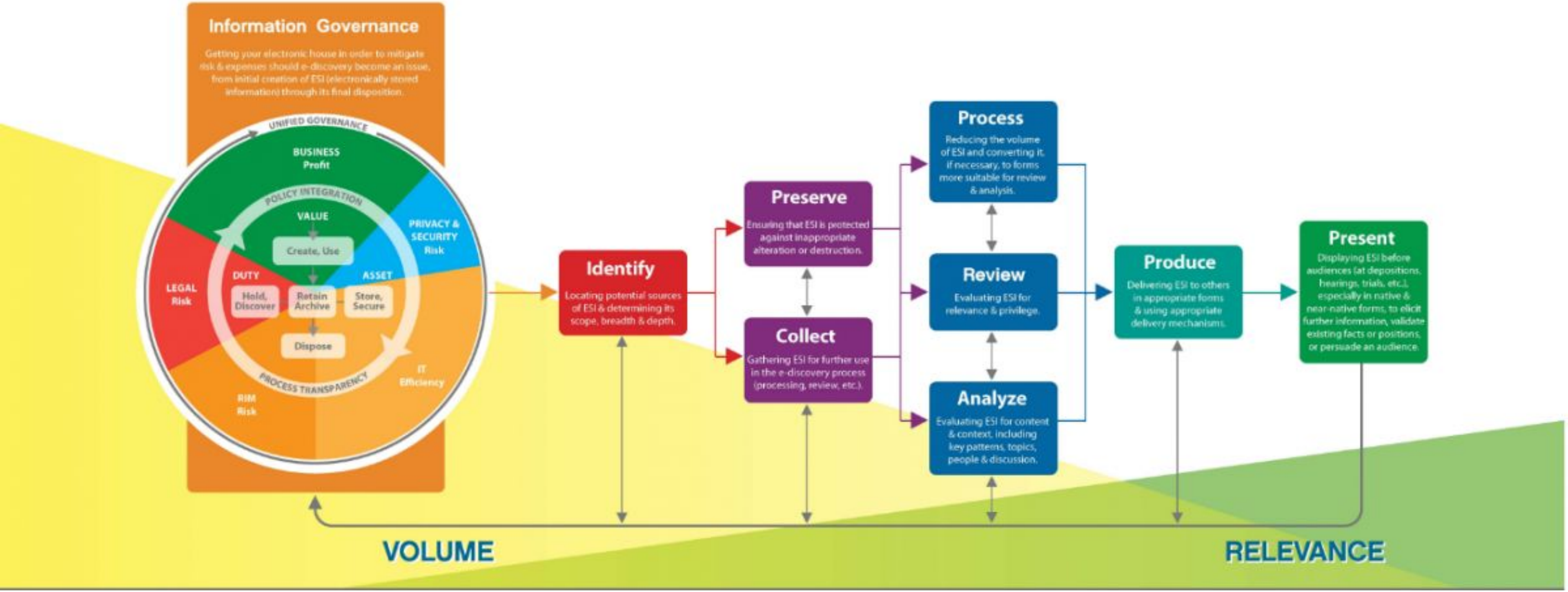
ESI - Electronically Stored Information

E-discovery, eDiscovery or Electronic Discovery.

LINK TO THIS POSTER:
https://edrm.net/resources/frameworks-and-standards/edrm-model/edrm-diagram-elements/

Electronic Discovery Reference Model

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



Information Governance

Getting your electronic house in order to mitigate risk & expenses should e-discovery become an issue, from initial creation of ESI (electronically stored information) through its final disposition.

Identify
Locating potential sources of ESI & determining its scope, breadth & depth.

Preserve
Ensuring that ESI is protected against inappropriate alteration or destruction.

Collect
Gathering ESI for further use in the e-discovery process (processing, review, etc.).

Process
Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.

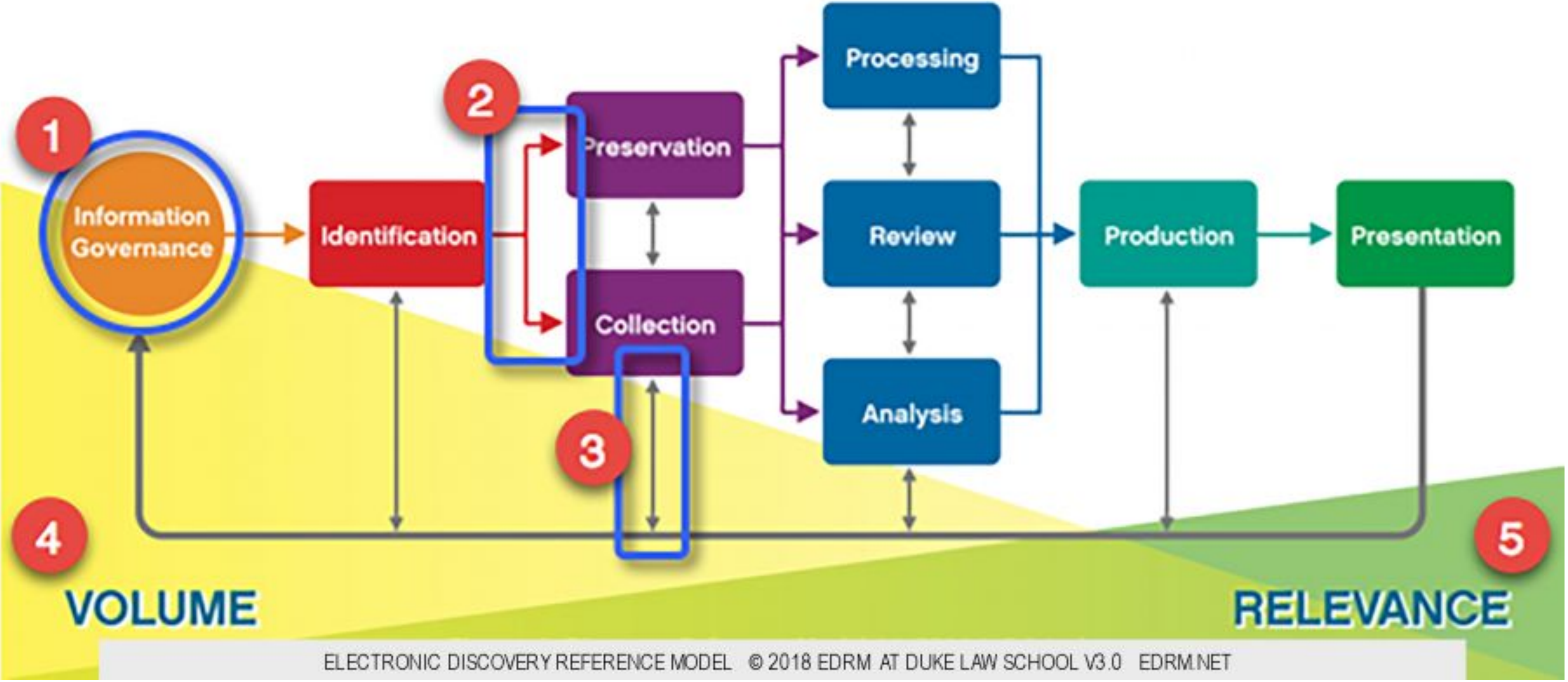
Review
Evaluating ESI for relevance & privilege.

Analyze
Evaluating ESI for content & context, including key patterns, topics, people & discussion.

Produce
Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.

Present
Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

Electronic Discovery Reference Model



ELECTRONIC DISCOVERY REFERENCE MODEL © 2018 EDRM AT DUKE LAW SCHOOL V3.0 EDRM.NET

Evidence

- **Proof** is a fact that demonstrates something to be real or true.
- **Evidence** is information that might lead one to believe something to be real or true.
- **Proof** is final and conclusive.

Crime Committed→ Facts, traces left behind→ Investigation Occurs→ Evidence Discovered → Help us Prove → Proof

Types of Evidence

Real

Documentary

Testimonial

Types of Evidence

Evidence must be Admissible

- ***Relevant*** to the Case
- ***Related*** to the Case
- ***Competent*** (Legally Obtained)

Main Types:

Real : Object Evidence → *Conclusive Evidence*, Incontrovertible (not able to be denied or disputed)

Documentary : Paper Records, Logs → *Best Evidence* , Not Copies

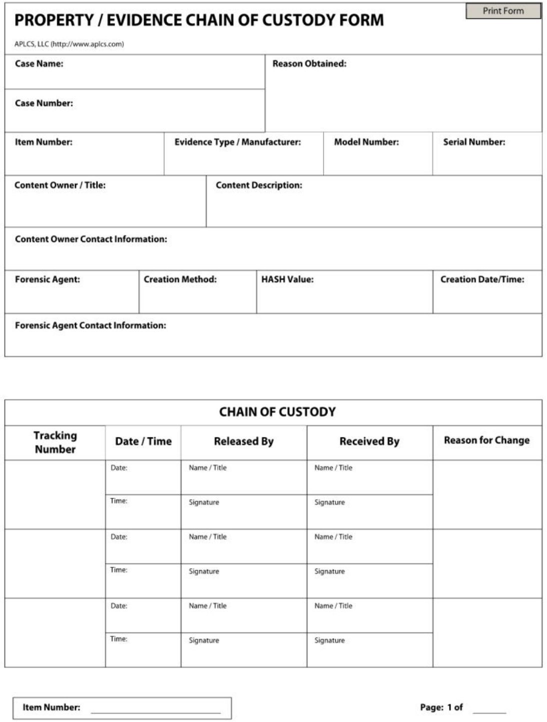
Testimonial: Testimony of a Witness → *Direct Evidence* , from Direct Observation
→ *Hearsay Evidence*, something they heard or something they saw.

Evidence Collection

Analytics:

Media Analysis- Hard Disks, Tapes, CDs, DVDs, USB, RAM and Solid State Drives)
Network Analysis - IDS, IPS - Logs, Pcaps, FW Logs
Software Analysis - Log files from Databases, or Event Logged. It could also be more advanced, such as Review of Software Code.
Hardware Device Analysis- Smartphones, Tablets, Computers, Embedded systems in Cars, Security Systems etc,

Chain of Custody



Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:

Case Number:

Reason Obtained:

Item Number:

Evidence Type / Manufacturer:

Model Number:

Serial Number:

Content Owner / Title:

Content Description:

Content Owner Contact Information:

Forensic Agent:

Creation Method:

HASH Value:

Creation Date/Time:

Forensic Agent Contact Information:

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date: Time:	Name / Title Signature	Name / Title Signature	
	Date: Time:	Name / Title Signature	Name / Title Signature	
	Date: Time:	Name / Title Signature	Name / Title Signature	

Item Number: ____________________

Page: 1 of ______

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	

Item Number: ______________________

Page: 1 of ______

ISC2 Code of Ethics

Code of Ethics Preamble:

The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

Act honorably, honestly, justly, responsibly, and legally.

Provide diligent and competent service to principals.

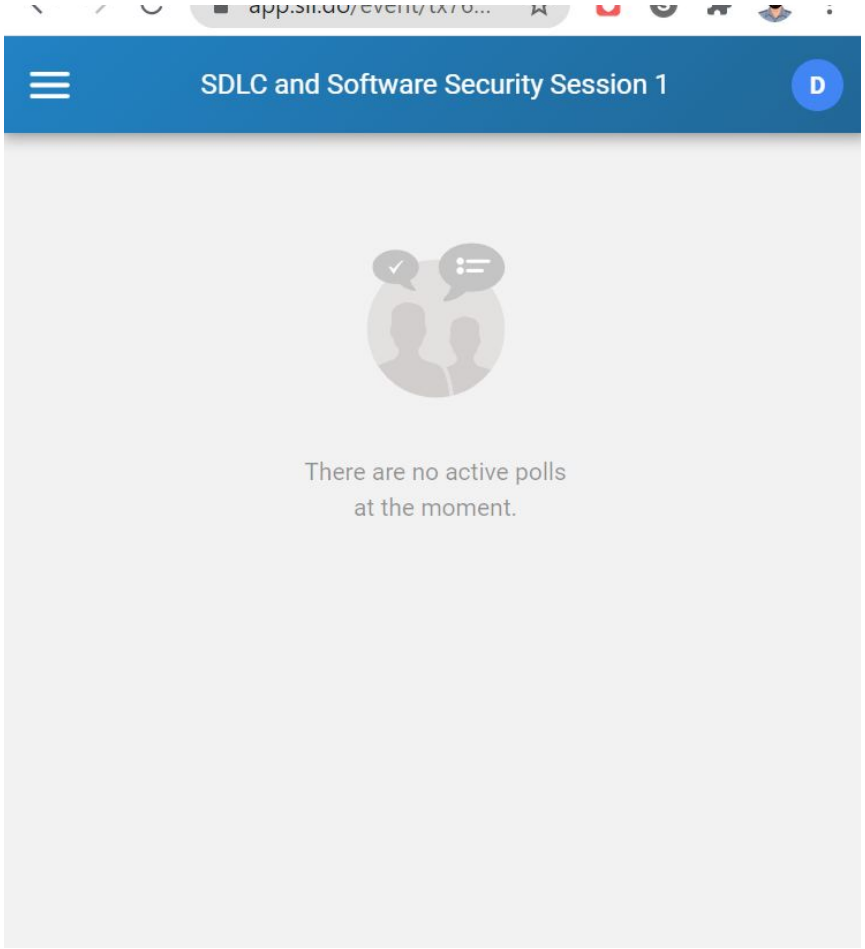
Advance and protect the profession.

Important Aspect of Each ISC2 Cannon

1. Protect the society
2. Be Lawful and Act Honorably
3. Be a Lawful and Honorable Professional
4. Protect the Certification and Profession

Quiz Time!

Please use another Device - Phone or PC



SDLC and Software Security Session 1

There are no active polls at the moment.

Go to

https://icsbits.com/go/cisspjam

Quiz will start once everyone has been able to join.

NOTES

Notes for this session and Old Sessions:

http://icsbits.com/go/notes

Thank you.

For notes and powerpoint go to

icsbits.com/go/notes