

ITS 833: Lecture 4

Week #4 Activities

- Learning Materials
 - 1- Read Ch.8 and 9 in the textbook
 - 2- Check the additional information at the end of this lecture
 - 3- Check the follow up questions and resources that I will post in discussion forums
- Assignment
 - 1- Answer week 4 discussion questions 1 & 2
 - 2- Provide feedback to other students' answers
 - 3- Complete midterm exam by end of coming Sunday

This exam would require 1 hour to complete,
You have only (2) attempts to complete.
It equals 20% of your final Course grade.
The exam covers ALL the chapter materials that we have covered (Ch. 1-9).
The exam has a total of 30 multiple-choice questions
- Discussion Time requirements
 - 1- Answer Q1 by Wednesdays
 - 2- Answer Q2 by Fridays
 - 3- Response to at least two students' answers for question 1 by Saturdays
 - 4- Response to at least two students' answers for question 2 by Saturdays

Last Week- Chapter 6

Information Governance Policy Development

- Chapter 6 presented and discussed major information governance (IG) frameworks and models,
- Explained IG Reference Model
- Explained IGRM Diagram
- Explained the best practice considerations when implementing IG Policy
- Discussed the benefits and risks of having IG standards
- Discussed the key standards relevant to IG

Last Week - Chapter 7

Business considerations for a successful (IG) program

- Discussed challenges of unstructured data
- Discussed Information cost models
- Discussed the key factors driving information costs

Lecture#4 Outline

- Chapter 8 key points
- Chapter 9 key points

Chapter 8: IG and Legal Functions

- Discusses how IG impacts legal functions within an organization
- Discusses the e-discovery techniques
- Explains the e-discovery reference model
- Discusses the Federal Rules of Civil Procedure (FRCP)
- Explains the benefits of a record retention policy
- Discusses the predictive coding
- Explains a record retention policy
- Explains the steps to defensible disposition of information

E-Discovery

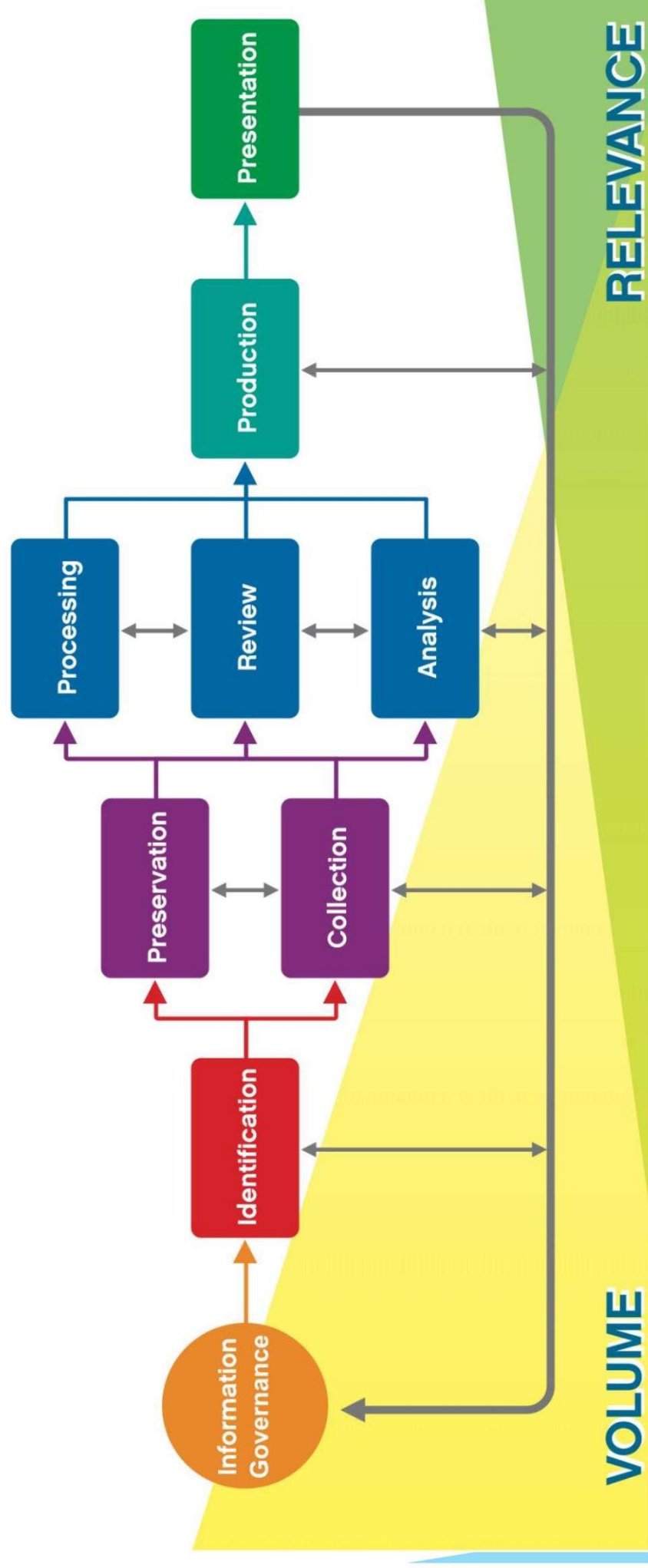
- Electronic discovery (e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.
- E-discovery can be carried out offline on a particular computer or it can be done in a network.
- Court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery
- In the process of electronic discovery, data of all types can serve as evidence. This can include text, images, calendar files, databases, spreadsheets, audio files, animation, Web sites and computer programs.

Electronic Records Legality Issues

- Electronic records can be accepted or rejected as evidence in court.
- A government's records must be:
 - authentic
 - accurate
 - trustworthy

E-Discovery Reference Model (EDRM)

- The Electronic Discovery Reference Model (EDRM) is a framework that outlines standards for the recovery and discovery of digital data.
- The EDRM is designed to serve as guidance for gathering and assimilating electronic data during the legal process, including criminal evidence discovery.



Predictive Coding

- Predictive coding is a technology that assists document reviewers during the review phase of a case. It reduces the total number of documents that a legal team needs to review by finding the set of documents that are relevant to the case.
- Typically it uses machine learning to label documents after the reviewers have completed some review, creating a “seed set” of coded (or labelled) documents.
- It improves the efficiency of human reviewers by understanding how they’ve labelled documents and then using those criteria to apply labels to documents that have not been reviewed yet.
- Technology Involved in Predictive Coding
 - Machine learning and artificial intelligence technology
 - Text analytics and word search
 - Pattern matching

Destructive Retention Program

- Records are destroyed under a records retention program when they are no longer needed for any legal, user, historical or other purpose.
- Records are also destroyed after microfilming or scanning as part of an electronic imaging system.
- Courts expunge records to eliminate any traces of an event such as an arrest or criminal conviction.
- The destructive program defines:
 - When does records destruction occur?
 - How should you legally destroy records?
- Retention Period: The minimum time that must pass after the creation, recording or receipt of a record, or the fulfillment of certain actions associated with a record, before it is eligible for destruction
- Destructive Retention Program is applied for electronic and non-electronic records

Defensible Disposition of Information Steps

- Explain the defensible disposition policy and get buy-in from stakeholders.
- Stakeholders need the opportunity to make their case for keeping some data beyond the mandatory deletion time
- Stakeholders need to approve the destruction of data they control.
- Check for any holds on data or exceptions to your rules.
- Document how much data you start with.
- Understand what data is covered by regulations or may have legal exposure issues
- Identify data disposition targets.
- Define disposition guidelines.
- For example, unstructured data like email messages may need to be moved to a searchable archive after six months and deleted at a defined later date. Your guidelines should include justification for all decisions, particularly exceptions.
- Create a records retention schedule.
- Denote the length of time each item should be retained at the finest level of detail possible.

Defensible Disposition of Information Steps

- Create a metadata tagging scheme.
 - Tagging data at its time of origin will make the ongoing disposition process much easier.
 - Choose tags that match your guidelines and any regulatory requirements.
- Conduct an information audit.
 - Locate and catalog the information you have.
 - Be prepared to apply technology tools to the task
- Delete and document.
 - Use a certified data destruction vendor with secure facilities that can provide certificates of destruction.
- Keep these documents in a secure place in case they're needed for legal defense or verification.
- Implement ongoing policies

Chapter 9: IG, Records, and Information

Management Functions

- Chapter 9 explains records and information management (RIM) functions of information governance (IG).
- Records and information management (RIM) defines the management responsible for the efficient control of creation, receipt, maintenance, use, and disposition of record (such as data, electronic documents, and reports)
- Electronic records management (ERM) has moved to the forefront of business issues with the increasing automation of business processes and the vast growth in the volume of electronic documents and records that organizations create.
- ERM systems must have complete retention and disposition capabilities.
- Implementing ERM is challenging as it requires user support and compliance, adherence to changing laws, and support for new information delivery platforms like mobile and cloud computing

Chapter 9: IG, Records, and Information

Management Functions

- Chapter 9 explains why Records Management is Challenging?
- Benefits of Electronic Records management
- Inventory E-Records process, purposes, principles, and steps
- E-Records Inventory Challenges
- Ensuring adoption and compliance of RM policy
- Developing a Records Retention Schedule
- General principles of Retention Scheduling
- Why are Retention Schedules needed?
- Retention of E-Mail Records
- How long should we keep old e-mails?
- Implementation of Retention Schedule and Disposal of Records

Additional Resources for Ch. 8 and 9

- E-Discovery 101: Gain a solid understanding of the basics
<https://www.youtube.com/watch?v=gUdQAIGxJ5Y>
- Introduction to E-discovery and Digital Evidence
<https://www.youtube.com/watch?v=btfcf9Hylns>
- E-Discovery Practices & Processes
<https://www.youtube.com/watch?v=WW4YBQvSCp0>
- Accelerating Investigations Using Advanced eDiscovery Techniques
<https://www.youtube.com/watch?v=0NoF4cpKzTw>
- Record Keeping and Record Retention
<https://www.youtube.com/watch?v=BcQ3n7okBeY>

Additional Resources for Ch. 8 and 9

- Document Retention Policies, Litigation Holds, and Legal Ethics
<https://www.youtube.com/watch?v=yE0IRWLOTqY>
- Regulatory Information Management (RIM)
https://www.youtube.com/watch?v=zKN09_hd2D8
- How to create a Retention Policy
<https://www.youtube.com/watch?v=EKKOeHQScX8>
- Electronic Records Labeling and Destruction Methodology
<https://www.youtube.com/watch?v=esz9QIdnJWY>
- Understanding Compliance and Records Management in Office 365
<https://www.youtube.com/watch?v=Sv1Pt0DiEDw>

Questions

- Student questions/comments related to the course: Student Question Forum
- Student personal questions/comments: Emails
- Email: Mohamed.Meky@ucumberlands.edu
- Expect my feedback: 1-24 hours