ITS 833: Lecture 5

Week #5 Activities

- Learning Materials

  1- Read Ch. 10 and 11 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 5 discussion questions 1 & 2

  2- Provide feedback to other students' answers

- 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 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

Last Week-Chapter 9: IG, Records, and Information Management Functions

- Records and information management (RIM) functions of information governance (IG).
- 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

Lecture#5 Outline

- Chapter 10 key points
- Chapter 11 key points

Chapter 10: Information Governance and Information Technology Functions

- Discuss the steps of implementing an effective data governance program
- Define the information management components and master data management (MDM)
- Explain the Information lifecycle management
- Define the data modeling
- Explain the different approaches to data modeling
- Explain several IT governance frameworks
- Best practices for database security and compliance

Steps of implementing an effective data governance program (page 192)

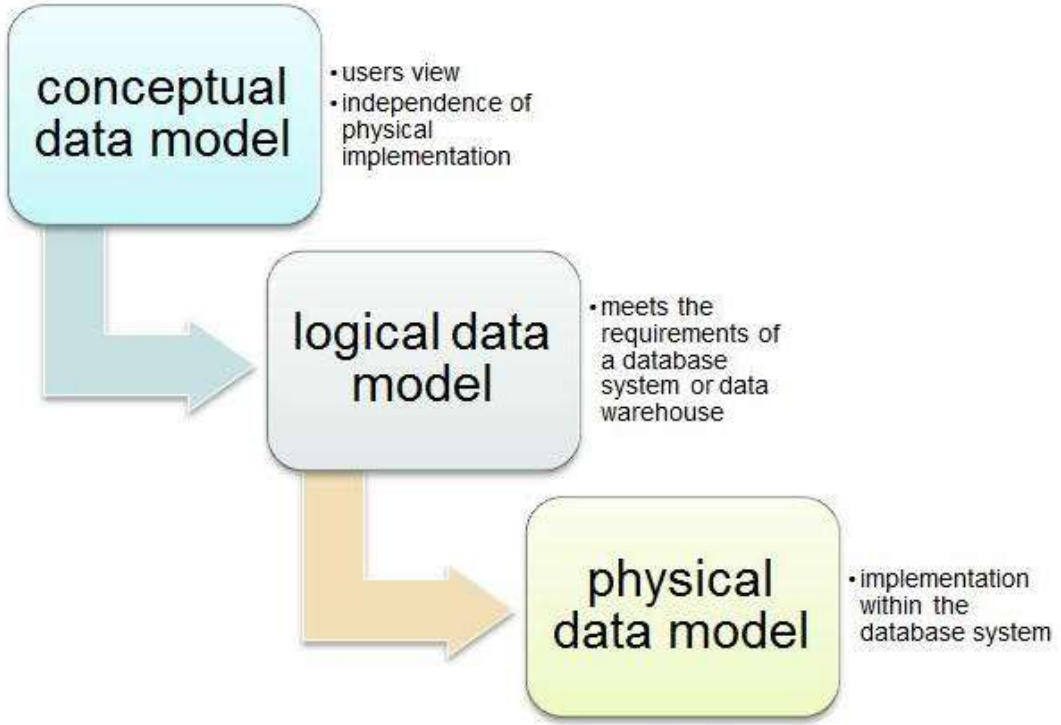
- Recruit Strong Executive Sponsor
- Assess Current State
- Set ideal state vision and strategy-Create
- Compute the value of your data
- Assess risks
- Implement “going forward” strategy
- Assign accountability for Data Quality to Business Unit
- Manage the Change
- Monitor Data Governance Program

Components of Information Management

- Master Data Management (MDM)-Goal is to ensure reliable, accurate data from a single source is leveraged across business units.
- Information Lifecycle Management – Managing information appropriately and optimally at different stages of its useful life
- Data Architecture – Design of structured and unstructured information systems in an effort to optimize data flow
- Data Modeling-Illustrates the relationship between data

Six Approaches to Data Modeling

- Conceptual data modeling – diagrams data relationships at the highest level
- Enterprise data modeling – business-oriented approach that includes requirements for the business or business unit
- Logical data modeling – Illustrates the specific entities, attributes and relationships involved in the business function
- Physical data modeling – implementation of a logical data model
- Data Integration – merges data from two or more sources, processing data and moving it into a database
- Reference data management modeling – refers to data in categories using look up tables, categorizes data found in a database – often confused with MDM



IT Governance Frameworks

- CobiT
- CobitT 5
- ITIL
- ValIT®
- ISO38500

Best Practices for Database Security and Compliance

- Inventory and document
- Assess exposure and weaknesses
- Shore up the database
- Monitor
- Deploy monitoring and auditing tools
- Verify privileged access
- Protect sensitive data
- Deploy masking
- Integrate and automate standardized security processes

Chapter 11: Information Governance Privacy and Security Functions

- Privacy Laws
- Insider attacks vs outsider attacks
- Limitations of traditional security
- Defense in depth concept
- Controlling Access Management (IAM)
- Challenges of security confidential e-documents
- Information Rights management (IRM) and its role in securing e-documents
- Data Loss Prevention (DLP) Technology

Privacy Laws

- Federal Wire Tapping Act
- Electronic Communications Privacy Act of 1986
- Stored Communications and Transactional Records Act
- Computer Fraud and Abuse Act
- Freedom of Information Act

Insider Threat

- Published in July 2012 on the insider threat in the U.S. financial sector gives statics on insider threat incidents within US firms:
  a. 80% of the malicious acts were committed at work during working hours
  b. 81% of the perpetrators planned their actions beforehand
  c. 33% of the perpetrators were described as "difficult employees"
  d. 17% as being "disgruntled.
- The insider was identified in 74% of cases and financial gain was a motive in 81% of cases, revenge in 23% of cases, and 27% of the people carrying out malicious acts were in financial difficulties at the time (Cummings, et al, 2012).

Refernece

- Cummings C, Lewellen T, McIntire D, Moore A,Trzeciak R (2012) Insider Threat, Security and Survivability. Software Engineering Institute. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=27971

DEFENSE IN DEPTH TECHNIQUES TO SECURITY

- Use Multiple Layers of Security Solutions
  - Firewall
  - Antivirus/antispyware software
  - Identity and Access Management (IAM)
  - Hierarchical passwords
  - Intrusion Detection
  - Biometric Verification
  - Physical Security
  - Security polices
  - Employee training
  - Auditing and monitoring

Protecting an Organization from Insider Threats

- Besides implementing defense in depth concepts, organizations should apply additional mechanisms to reduce the risk associated with employee's misbehave and insider attack. These additional mechanisms include applying least privilege, separation of duty, and rotation of duties concepts.
- Least privilege will limit access a user will have and prevent the user from potentially being able to access another application, data or system that he/she may not has access to.
- Separation of Duties (SOD) requires that no one person will have complete control or access to all applications. SOD will prevent the administrators from using the application as a way of committing fraud and other malicious acts.
- Rotation of Duties can be another way of preventing fraud. Rotation of Duties, similar to SOD, will be beneficial as an extra source of preventing fraud. The tasks for users will be rotated so that one person cannot have control of an entire application.

Security Limitations of Repository-Based Approaches

- In traditionally repository-based solutions, document saved in database servers/email servers located behind a firewall.
- Firewalls and access control models can grant or deny access to documents. However, it cannot define what users can and can't do with confidential data.
- We need better technology for protecting confidential data in the extended enterprise environment

Apply Better Technology for Better Enforcement In the Extended Enterprise

- Stop all extended access to confidential e-documents
- Implement secure printing
- Implement E-mail encryption
- Use digital signature
- Use data loss prevention (DLP) Technology to ensure that sensitive data does not exit through the firewall
- Use Information Right Management (IRM) technology
- Combining IRM and DLP technologies is the best available approach to securing e-documents and data.
- The use of thin-client and thin-device architecture can reduce security threats to confidential information
- Add auditing and monitoring capabilities to the access, use, and printing of documents
- Use document labelling to increase user awareness about the sensitivity of information in a document

Additional Resources

- The Journey and Roadmap to a Data Governance Program

https://www.youtube.com/watch?v=oTd9RwblaD4

- MER Conference: End-to-End Governance - Future-Proofing Digital Information

https://www.youtube.com/watch?v=qd7HtvBxL-s

- Webinar: Data Modeling & Metadata Management

https://www.youtube.com/watch?v=jyva44uHoR4

- The Convergence of Data Modeling and Data Governance

https://www.youtube.com/watch?v=AEecCrRWvR8

- Metrics that Matter - Top Reports for Database Security and Compliance

https://www.youtube.com/watch?v=vvuSmEgBjLYv

- How to Successfully Implement Info Security Governance

https://www.youtube.com/watch?v=RjzFDi6_2j8

Additional Resources

- Issues of Quantifying Risk around Identity and Access Management (IAM)

https://www.youtube.com/watch?v=vXwpxaYzAoc

- AWS IAM Tutorial | Identity And Access Management (IAM)

https://www.youtube.com/watch?v=UqKWHZ36yEM

- FileTrail Demo: Physical Records Compliance - Enforce Information Governance Policies

https://www.youtube.com/watch?v=yQG5nmKFEc8

- Overview of Data Loss Prevention (DLP) in Office 365

https://www.youtube.com/watch?v=S4YYVB-wpsE

- The Insider Threat is Real with Cybersecurity Expert

https://www.youtube.com/watch?v=z-CDyZdcGck

- Privacy vs. Security?

https://www.youtube.com/watch?v=bibcPiWgHIo

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