Study Objectives

- Auditing Systems Development, Acquisition and Maintenance – Recap
- Business Application Systems
Auditing Systems Development, Acquisition and Maintenance

• All phases of SDLC
  – Feasibility, Requirements, Design, Development, Testing, Acquisition, Implementation, Post Implementation
  – Pages 219-221 (CISA Review Manual 2014)

• Auditing involves
  – Risk Analysis of SDLC Phases (and also application & processes)
  – Identifying Major Gaps and Addressing them
  – Creating Reports and working collaboratively with the stakeholders
  – Follow-ups on action items
Business Application Systems

• eCommerce and EDI System – Discussed Before (week 6 – Revisit)
e-Commerce Application – Functionality (week 6)

- Allows commerce through the web-sites
- Typical Models
  - B2C (Business to Consumer)
    - A self-service channel for Consumers interacting with the Business
    - Could have a sales, service, information-sharing goals
    - Payments related transactions (could be part of sales, service)
    - Recent advancements: music, video streaming, games, entertainment hub
  - B2B (Business to Business)
    - For suppliers and partners
    - Information sharing, communication of information
    - Shared application components
  - Other models
    - B2E (Business to Employee)
    - B2G (Business to Government)
    - C2G (Consumer to Government)
    - X2X (Exchange to Exchange)
E-Commerce – Components Example (week 6)
e-Commerce Application – Architectural components (week 6)

• Authentication and authorization
  – Ex. Users access management to the site, what they can do (B2C)
  – Authentication, password, and communication components (B2B)

• Application Functionality
  – The core functionality of the e-Commerce application

• Product Catalog
  – E-Commerce site should allow easy configuration of products, information about products, their pricing, promotion to be managed
  – Easy display and change of the look and feel of the site to improve usability, sales, and service. Ex., through CMS

• Ordering
  – Managing shopping experience, shopping cart

• Service
  – Managing customer issues
  – Related to enterprise services or related to shopping etc
  – Ability to Chat for help
e-Commerce Application – Architectural components contd. (week 6)

• Payments
  – Various ways payments can be processed and handled
  – Credit card, PayPal, Debit from bank-account
  – PCI (Payment Card Industry) standards

• Reporting
  – Logging of relevant transactions
  – Operational reports for the transaction
  – BI (Business Intelligence)
  – Performance tracking
  – Ex HP BAC, Adobe Omniture, Google Analytics

• Feedback from Customers
  – Great opportunity for Business to collect customer feedback
  – Helps improve the site

• Etc...
E-Commerce Application IT Controls (week 6)

- COBIT seven information criteria for Application systems, could be a good framework to assess e-Application Controls
  - Primary
    1. Availability
    2. Effectiveness
    3. Compliance
    4. Confidentiality
    5. Integrity
  - Secondary
    6. Efficiency
    7. Reliability
1. **Availability:** The system needs to be highly available in general. 24X7 typical.
   - Capacity planning, redundancy, active-active, failover consideration
   - Ability to do seamless change management without affecting customers, sites, or transaction

2. **Effectiveness:** Making sure intended business function is met
   - How well supported is the critical business functionality? Fall-out handling, say for the orders
   - Audit trails
   - Content Management Process: should be controlled
   - Typical Input, output, and processing controls
   - Integration with back-end processes and Application is important

3. **Compliance:** with Regulations and Best Practices
   - Regulatory compliance
   - Authentication and Authorization

4. **Confidentiality:** Data protection consideration
   - Privacy and data protection consideration (ex, collecting and handling PII information)
5. **Integrity**: Integrity of the systems and data
   - Non-repudiation
   - Communication controls between the system components
   - Security Consideration important for e-Commerce applications
     - External threats including denial of service, unauthorized access to data, and unauthorized access of computer
     - Virus protection
     - Firewall, ACL controls
     - Cryptography such as proper use of https, SSL for communication
     - Digital signature so the initiator can be uniquely identified
     - Infrastructure controls to have valid digital certificates. Certification Authority (CA) and Registration Authority are involved
     - Encryption of data at rest

6. **Efficiency**: How well the functionality performing?
   - Response time
   - Workflow and fulfillment

7. **Reliability**: Ability to handle issues, downtime, etc.
   - Ability to bounce back from an issue
   - Performance under load
EDI (Electronic Data Interchange) – week 6

- Allows interchange of the documents between the partners
- Examples invoice, quotation, Order etc.
- EDI Process includes
  - Translation
  - Transmission
  - Storage of transactions
- Traditional EDI
  - Typically used by large corporations
  - Has typically 3 functions for each of the trading partners
    - Communication handler – process of transmitting and receiving electronic data between partners via dial-ups, dedicated lines, PSTN (public switched telephone network)
    - EDI Interface – interface function that manipulates and routes data between application systems and communication handlers. Composed of two components:
      - EDI translator: to translate data between standard format (ANSI X12) to trading partner’s proprietary format
      - Application Interface: to move the data to and from application system
    - Application System: systems that process data sent to or received from trading partners
- Web-based EDI
  - Takes advantage of the data transmission through internet
  - Improvement in the x.12 EDI formatting standards
EDI – Components Example – week 6
EDI Application IT Controls Consideration – week 6

• Encryption: to ensure authenticity, integrity, confidentiality of data

• Authentication: to ensure the trading partner ensure validity of the source and destination

• Transmission Controls: completeness and accuracy
  – Edit checks to identify erroneous and invalid transactions
  – Logging of the data
  – Counts, hashes, etc.
  – Authority of the account authorized

• Reasonableness check: for transaction validity
  – Control totals
Business Application Systems

• Textbook – CISA Review Manual
• Business Application Systems examples
  – Financial
  – Banking
  – CRM
  – Data Mining / BI
  – Etc…
Upcoming Assignments/Tests

1. Final (multiple choice questions 40-50 modeled after CISA exam. Covers entire course.): Mon 12/15

Questions?
Summary of Today’s Class

• Auditing Systems Development, Acquisition, and Maintenance

• Business Application Systems

No Next Class – Good Bye and Good Luck!