Study Objectives

• Group Project 1
  – Group Presentation
• Architecture and Design Phase (contd.)
  – Software Architecture
  – Client Server
  – Distributed
Group Project 1

Class Presentation and Discussion
Design Flow Diagrams

• There are a number of design diagrams designers use
• ER Diagram, Sequence Diagram (covered)
• DFDs (Data Flow Diagram) for structural decomposition of the system. Context diagram is highest level diagram of the system that can be further decomposed
  
  http://www.smartdraw.com/resources/tutorials/entity-relationship-diagrams/#/resources/tutorials/Introduction-to-DFD

• UML Diagrams
  – Class Diagram: describes static structure of the system
  – Use Case diagram: models functions of the system using actor and use cases
  – Sequence Diagram: interaction amongst classes across time
  – Collaboration Diagram: interaction amongst objects as sequenced messages
  – State Chart Diagram: behavior of the systems as its state changed
  – Activity Diagram: flow of control from activity to activity
  – Component Diagram: organization of physical components
  – Deployment Diagram: for deployment; refers to physical resources

  http://www.smartdraw.com/resources/tutorials.uml-sequence-diagram/#/resources/tutorials/Introduction-to-UML
UI Best Practice

User Interface Best Practice

1. Simple Navigation
2. Functionality - Do what is needed
3. Response Time
Question

Which of the following design techniques deals with internal functions used for data and process changes?

A. Function point analysis
B. ER diagram
C. Flowchart
D. Database Schema
Auditing Detailed Design and Architecture

• Review system architecture to get an understanding of the architectural building block of the application such as UI, Process Layer, Data Layer
• Review flow-charts (process flow, data flow, ERD diagram, sequence diagrams etc. to ensure general adherence to the designs
• Verify the appropriate approvals were obtained from User Management
• Review that the appropriate input, processing, and output controls are designed into the systems during detailed design
• Ensure testing considerations have been included as part of the detailed design
• Ensure the design is traceable from the systems requirements and is complete
• Ensure that interface designs across the systems components are clearly identified
Auditing Detailed Design and Architecture contd.

- Ensure that security and system access design (authentication, authorization) is included in detailed designed
- Ensure hardware architecture (including Disaster Recovery, active-active consideration etc.) is included
- Verify that application operation requirements and incident management requirements are properly designed
- Interview User Management and Business team to determine their level of input into the design of screens, error handling, reporting etc. are included
e-Commerce Application - Functionality

• 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 Application – Architectural Considerations

• Two-tier architecture
  – Client browser and web-servers

• Three-tier architecture
  – Client browser, web-servers, database servers

• N-tier architecture
  – Client-browser, web-server, app-servers, database servers, content management servers (CMS), Reporting servers, back-end application interfaces including SOA layers,...
E-Commerce – Components Example
e-Commerce Application – Architectural components

- 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.

• 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

• 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
E-Commerce Application IT Controls

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)
E-Commerce Application IT Controls

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
Auditing Web Applications Check List
(Another Perspective)

1. Ensure web application is protected against injection attack
2. Check for cross-site scripting vulnerabilities
3. Review application for broken authentication and session management vulnerabilities
4. Verify for proper object reference and authorization
5. Verify control is in place to prevent Cross Site Registry Forgery
6. Review controls surrounding maintaining secure configuration
7. Verify secure cryptographic storage mechanisms being used
8. Verify control in place to restrict URL Filtering
9. Evaluate transport layer protection mechanism
10. Review web application redirects to ensure only valid URLs are accessible
11. Verify all inputs are validate prior to use by web server
12. Evaluate the use of proper error handling

Source: Adapted from “IT Auditing – Using Controls to Protect Information Assets”, Davis et. al.
EDI (Electronic Data Interchange)

- 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
EDI Application IT Controls
Consideration

- 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
Upcoming Assignments/Tests

1. Group Project -1 (Business Case, RFP): Tues 10/6 before the class
2. Individual Case Study -2 (Requirements and Use Case): Mon 10/20 before the class
3. Quiz 2 (Week 5 – Week 8): Mon 10/27

Questions?