Study Objectives

• Systems Implementation contd...
  – Configuration Management
  – Monitoring and Incident Management

• Post implementation Reviews
  – Project Success Criteria
  – Lesson Learned

• Secure SDLC
Configuration Management

• What’s the role of Configuration Management?

• Managing access to the program files such as source code to the authorized individuals (developers for code, for example)

• Prevent corrupting the program by accidentally overwriting by one user, when other user is also working on the same module

• Provide ability to “check out” and “check in”

• Provide ability to keep separate versions of the program to track the changes
Configuration Management

- What’s the role of Configuration Management?
- Managing access to the program files such as source code to the authorized individuals (developers for code, for example)
- Prevent corrupting the program by accidently overwriting by one user, when other user is also working on the same module
- Provide ability to “check out” and “check in”
- Provide ability to keep separate versions of the program to track the changes
Configuration Management

• Tools Used for Configuration Management
  – TFS (Team Foundation Server) in Microsoft Development Environment
  – CVS for Java Environment
  – Continuus

• Artifacts typically managed by a Configuration Management Tool
  – Code
  – Design
  – Configuration files
  – Test Scripts
  – Release Management Documentation
  – Reports
  – DDLs
Configuration Management Contd.

• Checking-out /Checking-in
  – An artifacts can be checked in in the Configuration Management Tool (version n)
  – Subsequent version must be checked out before changes can be made. Once the changes have been made and tested, the artifact can be checked back in as the next version (version n+1)

• Configuration Management Policy
  – Should be developed, and the process should be understood be the developers, designers, tester, etc.
Monitoring and Incident Management

- Monitoring deals with keeping an eye to the “vital signs” of the systems in production
- There can be different types of monitoring
  - OS and hardware monitoring
  - Database monitoring
  - Application monitoring
    - Response time
    - Error rate
    - Monitoring availability of the system
- Helps in the performance measurement of the project
Monitoring and Incident Management

• Incident Management ensures if an incident has occurred such as outage or a problem ticket is reported, the incident is properly handled and the problem is resolved in timely manner

• In the outage situation
  – various teams such as Level 1, Level 2, and Level 3 support should get engaged on as needed basis
  – Communication to the stakeholders including IT and Business Management and User community are notified in timely manner on the progress of resolution

• RCA (Root Cause Analysis) and Corrective Actions should be documented and followed-up on to avoid repetition of the similar incident
Auditing Implementation

- Review data conversion plan and test results to ensure proper conversion of data (accuracy and completeness)
- Review User-Acceptance plan, involvement of Users, and the results, to ensure user buy-in
- Ensure proper Change Management procedure has been in place to ensure Change has been documented, artifacts planned, and approved by stakeholders
  - test results, implementation steps, roll-back plan, etc. are there and previously tested
  - All the changes to the programs during the testing has been incorporated
- A “smoke” or mini-regression test is performed after the change to the programs has been frozen
- Review implementation approach and if that is appropriate (parallel changeover, phased changeover, abrupt changeover)
Auditing Implementation contd.

• Go decision has been made by the stakeholder (typically User Management, Business, Development, Testing, and Project Manager) as part of go/ no-go decision typically before the day of implementation

• Ensure a communication plan has been developed during implementation and after successful implementation

• Verify the best practices for implementation is in place such as
  – practice related to minimizing user impact
  – only authorized access to production environment to the Operation team (developers shouldn’t have access)

• Ensure production performance monitoring, incident management, and outage management processes are in place to address any production issues in timely manner
Questions

What kind of testing(s) is/are done as part of Software implementation?
A. Regression
B. Progression
C. UAT
D. Smoke
Questions

What kind of testing(s) is/are done as part of Software implementation?
A. Regression
B. Progression
C. UAT
D. Smoke
Post Implementation Review

• What is applicable to Post Implementation Reviews?

A. Conduct Lesson Learned Meetings
B. Assess the actual benefit of the project against the Business Case
C. Closing the project
D. Assign Open Action Items to the relevant teams
E. Fix the outstanding issues and conduct post-implementation reviews again and again until the project benefits are realized
Post Implementation Review

- What is applicable to Post Implementation Reviews?

A. Conduct Lesson Learned Meetings
B. Assess the actual benefit of the project against the Business Case
C. Closing the project
D. Assign Open Action Items to the relevant teams
E. Fix the outstanding issues and conduct post-implementation reviews again and again until the project benefits are realized
Steps for Post Implementation Reviews

1. Review Project Performance
   - Business benefits against business case

2. Review Project Conformance
   - Did the project meet the project plan?
   - Was the project delivered on time?
   - Was the project delivered on budget?
   - Was the project delivered with acceptable quality?
   - Did the project conform to the communication, change management, risk management, issue management, and vendor management goals

3. Identify project accomplishments
4. Identify major issues or failure
5. Identify Lesson Learned
6. Close the Project

Adapted from [http://blog.method123.com/2007/01/01/post-implementation-review/](http://blog.method123.com/2007/01/01/post-implementation-review/)
Benefit Realization Measurement

• Once the project is implemented Business Owner and IT Leaders typically collaborate to measure the benefits of the project
  – Benefit Cost analysis, NPV etc. are quantitative measures that can be computed over time
  – The benefit can be compared against original business goals
  – This analysis often helps in prioritizing new functionality or enhancements for future projects
  – Sometimes, if the benefit is not as thought initially to be, the management team can make a decision not to continue with the future phases of the projects
Project Conformance

• Against the planned goals within the standard Project Management areas

• Time, Budget, Quality are 3 major KPIs
These could be functional or process related
Could be quantitative or qualitative
Not restricted to financial goals
Lesson Learned Meetings

• Also called sometimes “post mortem”
• Development, Test, Business Partners, Users typically after a Release Implementation get together to
  – Discuss activities that went well
  – Pain areas and challenges
  – What can be done better
  – The topics include all areas including processes, communication, functional items, scope etc
  – The goal is to learn from each other and become better
• Action Items are often documented and managed by the Release Manager to be incorporated in the next or future releases
Closing a Project

• Typically after implementation of one or more releases of the project
• When project is implemented for most part and the benefit is realized, or when the project is implemented and benefits thought not to be as expected
• Major follow-ups can be recorded and provided to the key stakeholders
• The project team is disbanded
Post Implementation Reviews

Additional References

ITIL Library

Secure SDLC

• Secure SDLC – has a lot of emphasis today where Cyber Security is a key maturing discipline in organizations

• Spans all phases of SDLC
  – Agile: Secure SDLC user stories

• Training and Secure SDLC is a key area of focus

• Constant Vulnerability Management is Required
  – Code and System scanning
  – Remediation
Secure SDLC Applicable All Across Development & Operation

**Phase 1: Feasibility**
- Data Protection Requirement (sensitive, public, PII, etc.)
- Accessibility of system and data
- User Access
- Partner communication
- Reports
- Non-functional requirements
- Threat modeling

**Phase 2: Requirements**
- Infrastructure design
- System logic design – least privilege, logics on protected servers, tiered architecture
- Authentication / Password Management
- Cryptography
- Input validation / Output Encoding
- Session Management
- Access Control
- Error Handling and Logging
- Data Protection
- Communication Security
- Database Access
- File Access
- Memory management
- System configuration

**Phase 3: Design/Selection**
- Coding and UT
  - Developer training
  - Application of Secure Coding design principles
  - Static code analysis with the build
  - Secure coding modules such as for cryptography
  - Peer reviews

**Phase 4: Development/Configuration**
- Testing
  - Vulnerability scanning or penetration testing
  - Dynamic code analysis
  - Security Metrics

**Phase 5: Implementation**
- Tools
  - Threadfix
  - Dell Secureworks

**Phase 6: Post Implementation**
- Hardware/OS scanning
- Change Management controls
- Access to production systems using least privilege for hardware, network, OS, Services
- Firewalls across application tiers
- Multiple network zone

- Regular Production system scanning or penetration testing
- Vulnerability prioritization and mitigation
- Adherence to standards for cryptography, communication, etc.
- Access control reviews
Secure SDLC Further Read

- Secure Coding – Not just for code, but includes design concepts
  

- A good Secure SDLC presentation
  
Upcoming Assignments/Tests

1. Group Case Study -3 (Testing): Thu 4/14 before the class

2. Extra Credit for Class Participation: Choose your own topic. 3-5 pages of Report, Analysis, Design, etc within the domain of SDLC. Due: Thu 4/21 before the class. Send an email to Vasant with your work. Encourage you to submit a hard copy in the class as well. Note: As we discussed in the class on 4/7, this exercise is at request of some of you, and is OPTIONAL.

3. Final (multiple choice questions 40-50 modeled after CISA exam. Covers entire course.): Thu 4/28
   Note: We will use TU Classroom Exam Answer Sheet (bubble sheet). Bring your pencils in the class.

Questions?
Summary of Today’s Class

• Change Management
• Release Management
• Post Implementation Review
• Secure SDLC
• Focus of the Next Class and Reading
• Questions