Introduction to Change Management and SDLC

Steve Owyoung, Director, KPMG

Doug Mohrland, Audit Sr. Manager, Oracle

Core Competencies - Session C13

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Discussion Topics

- Significance of change management
- Types of changes
- Change management controls
- Leading practices
- Software Development Lifecycle (SDLC)

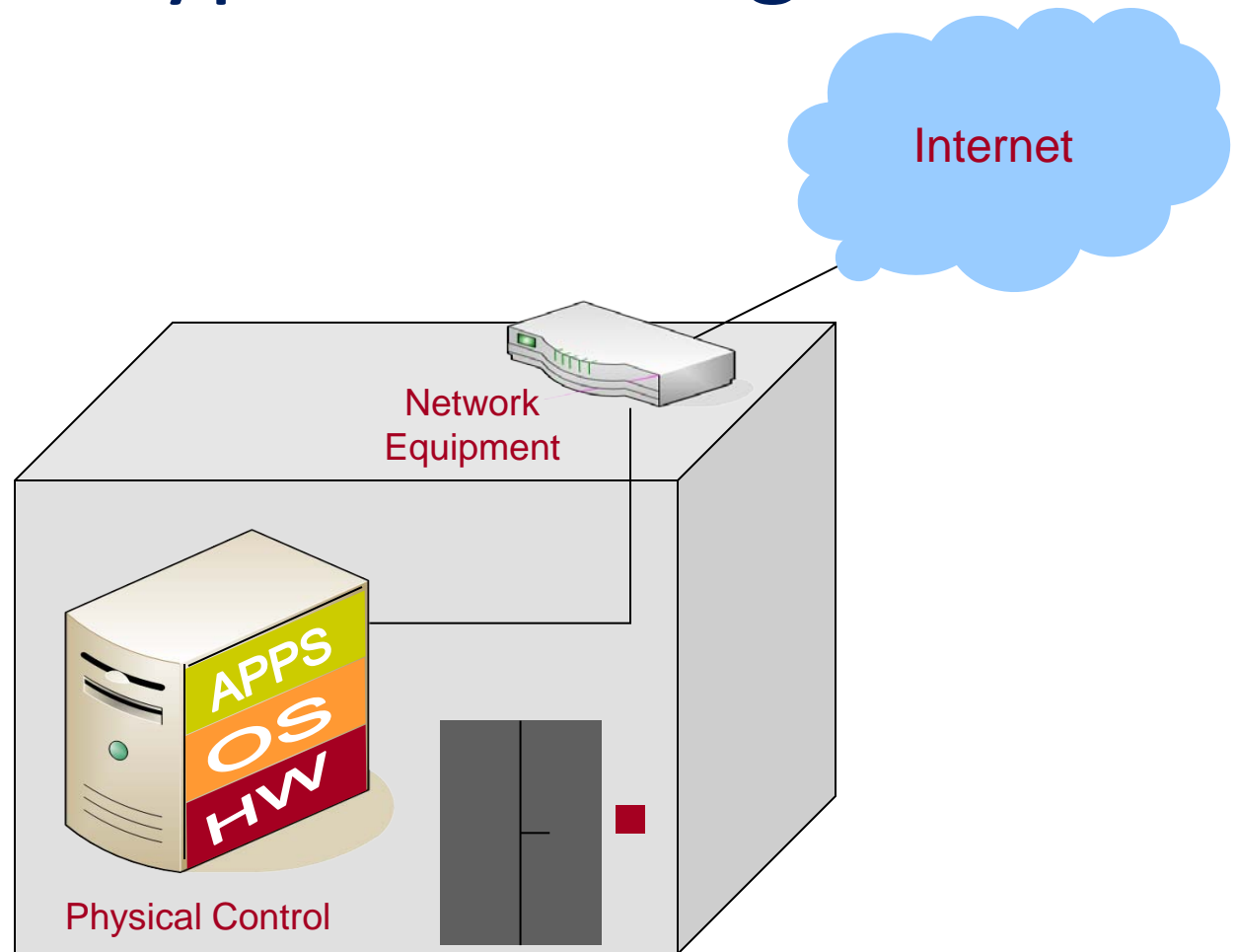# Significance of Change – What drives change in organizations?

Customer demand/need

Government

Competition

Technology

Constant Environment Change

Organization

Why change management and its significance?

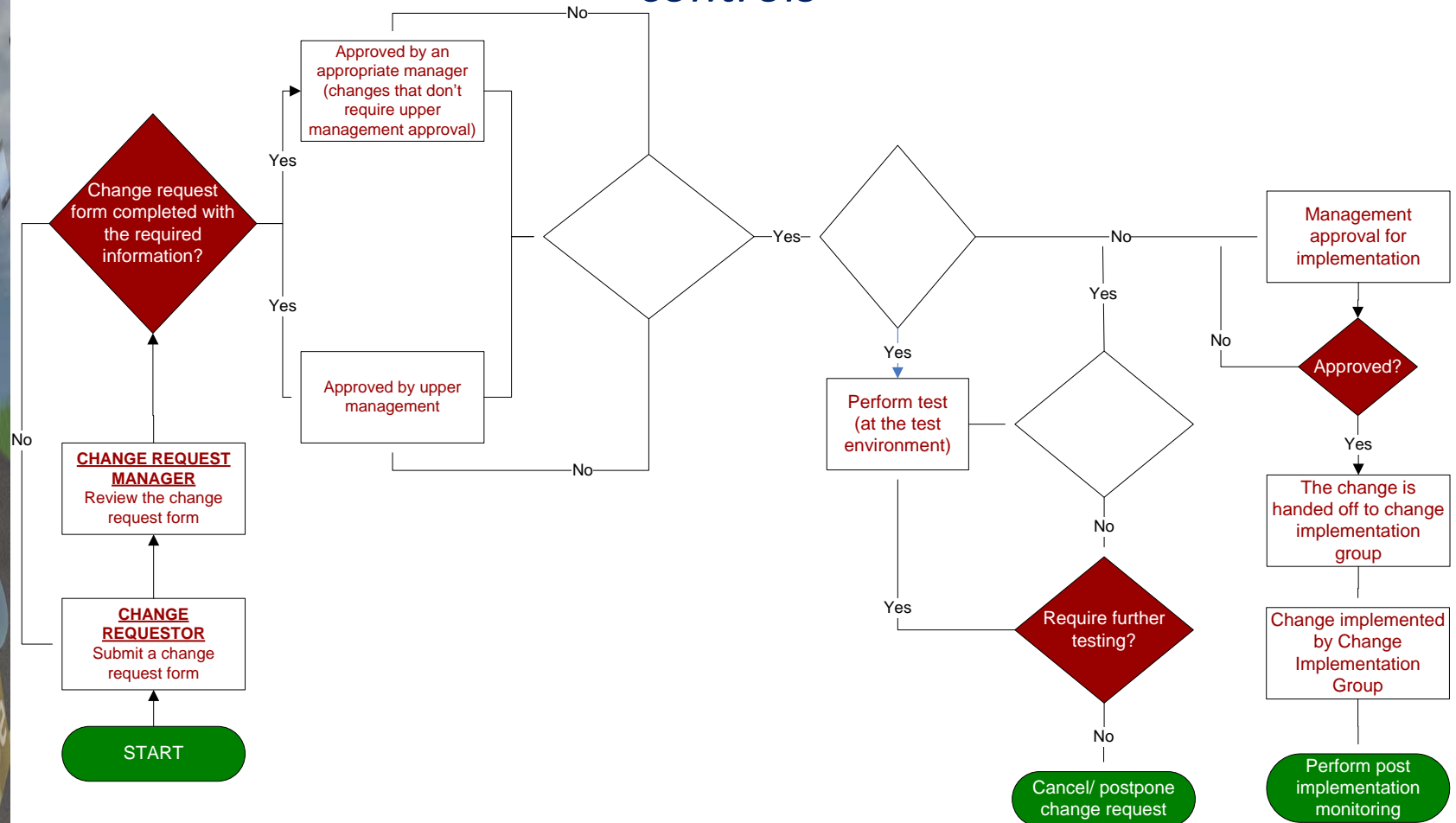Change management – it is significant because it helps an organization to be efficient

| Adapting to change | Controlling change | Effecting change |

Types of changes

Internet

Network Equipment

APPS
OS
HW

Physical Control

Refer to Appendix I for additional details.

Change management controls
Planned/routine maintenance changes procedure and controls

Flowchart:

- **START** → **CHANGE REQUESTOR** Submit a change request form → **CHANGE REQUEST MANAGER** Review the change request form → **Change request form completed with the required information?**
  - No → back to CHANGE REQUESTOR
  - Yes → Approved by an appropriate manager (changes that don't require upper management approval)
  - Yes → Approved by upper management
- Approved by an appropriate manager → decision diamond
  - No → (top route)
  - Yes → next decision
- Approved by upper management → No
- Decision diamond → Yes → Perform test (at the test environment)
  - No → Management approval for implementation
- Perform test → Require further testing?
  - Yes → back to decision
  - No → Cancel/ postpone change request
- Management approval for implementation → **Approved?**
  - No → (back)
  - Yes → The change is handed off to change implementation group → Change implemented by Change Implementation Group → **Perform post implementation monitoring**

Change management controls
Emergency/System Recovery change procedure and controls

EMERGENCY CHANGES
The change requestor solicits management approval (verbal is acceptable)

CHANGE REQUESTOR
Request a change (complete an Emergency Change Request Form)

Approved by management or by the staff managing the production systems? — Yes

Test required? — No

Notify all the constituents before production implementation

Implement change into production

No

Yes

The staff managing the production systems perform professional judjment and make a decision whether to proceed or cancel the emergency change

Perform testing (test environment) — Yes

Test passed?

No

Yes

The changes and the back out plans should be documented in the Change Request Form for later management review

SYSTEM RECOVERY
The production support staff immediately respond and start resolving the issue

Perform post implementation monitoring

Change management controls

- Maintain System Integrity:
  - Prevention
  - Detection
  - Correction/Recovery

Refer to Appendix II for additional details.

Change management leading practices

- Change management policy, procedure and standards
- Change request management
- Approval process
- Deployment management
- Change result management
- Monitor application and networks

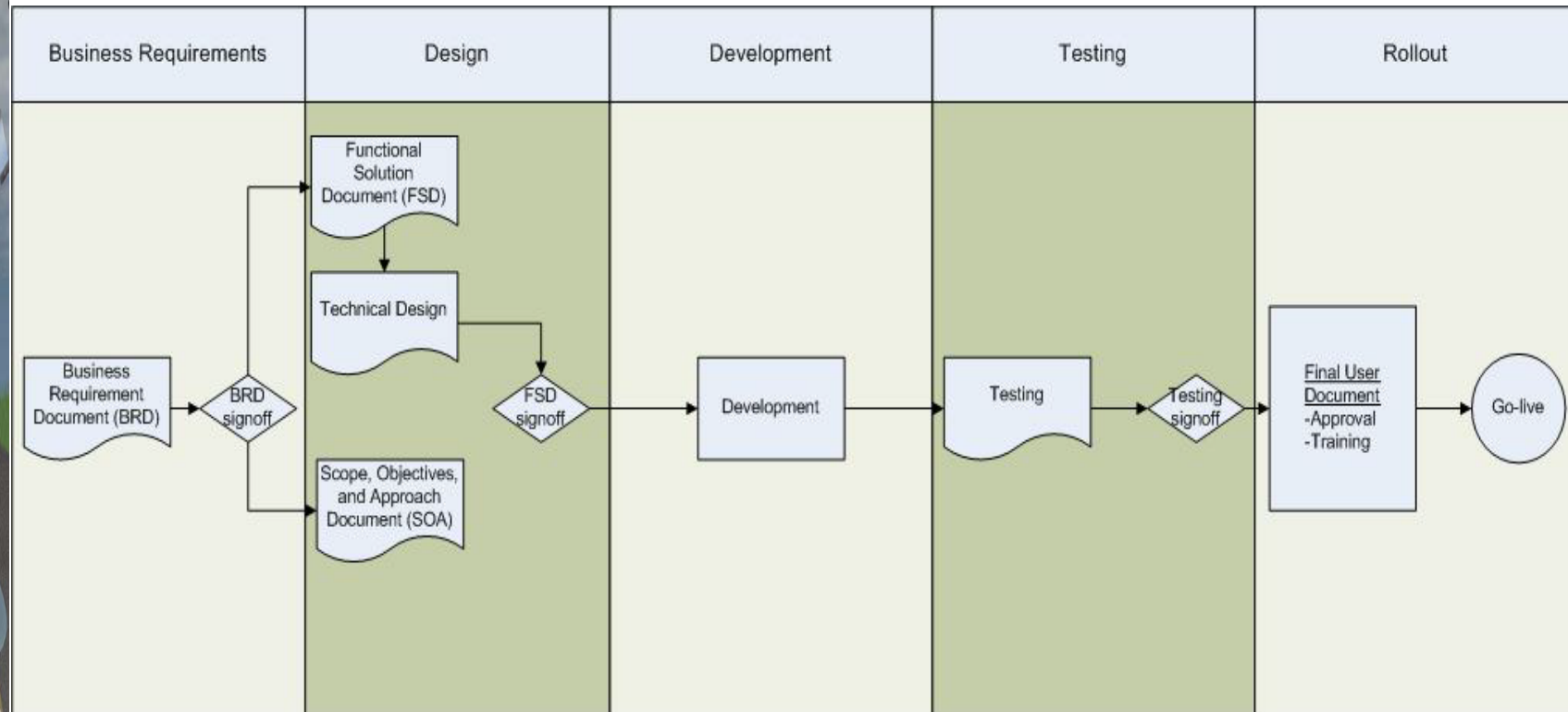Refer to Appendix III for additional details.

Software Development Life Cycle
Relationship between change management and SDLC

- Managing change is a critical component of any SDLC model
  - Change Management and SLDC are not mutually exclusive
- Change management occurs throughout the development life cycle
- Cost of changes is higher once out of development
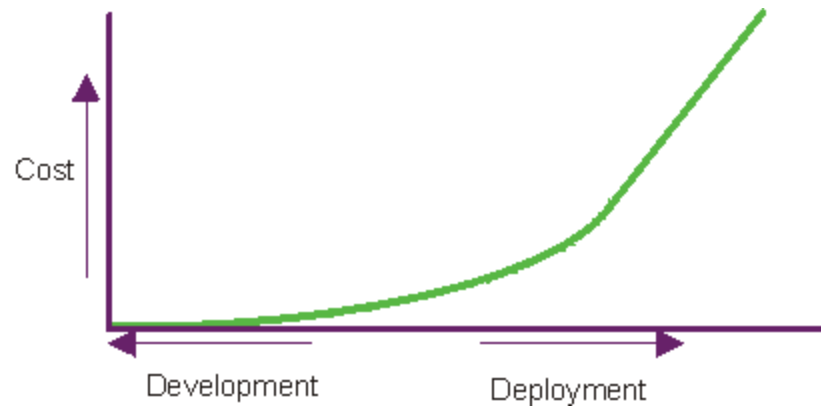
Software Development Life Cycle
Relationship between change management and SDLC

Business Requirements	Design	Development	Testing	Rollout

Business Requirement Document (BRD) → BRD signoff → Functional Solution Document (FSD) / Scope, Objectives, and Approach Document (SOA) → Technical Design → FSD signoff → Development → Testing → Testing signoff → Final User Document -Approval -Training → Go-live

Software Development Life Cycle
Testing Phase

Testing	Responsibility	Purpose
Unit/Component	Development Team	To isolate each part of the program and show that the individual parts function properly (Technical/Functional Spec)
Black Box	QA/Testing Team	To check if user interface and user inputs and outputs are as expected (Technical/Functional Spec)
White Box	QA/Testing Team	To test the internal structure and ensure functionality is working appropriately (Technical/Functional Spec)
Regression	QA/Testing Team	To ensure that a change, such as a bug fix, did not introduce new faults (Technical/Functional Spec)

Software Development Life Cycle
Testing Phase (cont.)

Testing	Responsibility	Purpose
Integration	QA/Testing Team	To ensure distinct components of the application still work in accordance to requirements (Functional Spec)
Performance/ Load	QA/Testing Team	To test the behavior of the application under a specific expected load (Functional Spec)
System	Customer, End Users	To evaluate the system's compliance with its specified requirements. (Business/Functional Spec)
Acceptance	Customer, End users	To determine if it meets their requirements (Business Req/Functional Spec)

Software Development Life Cycle
Relationship between change management and SDLC

- Waterfall model

Mange Change

SYSTEM REQUIREMENTS → SOFTWARE REQUIREMENTS → ANALYSIS → PROGRAM DESIGN → CODING → TESTING → OPERATIONS
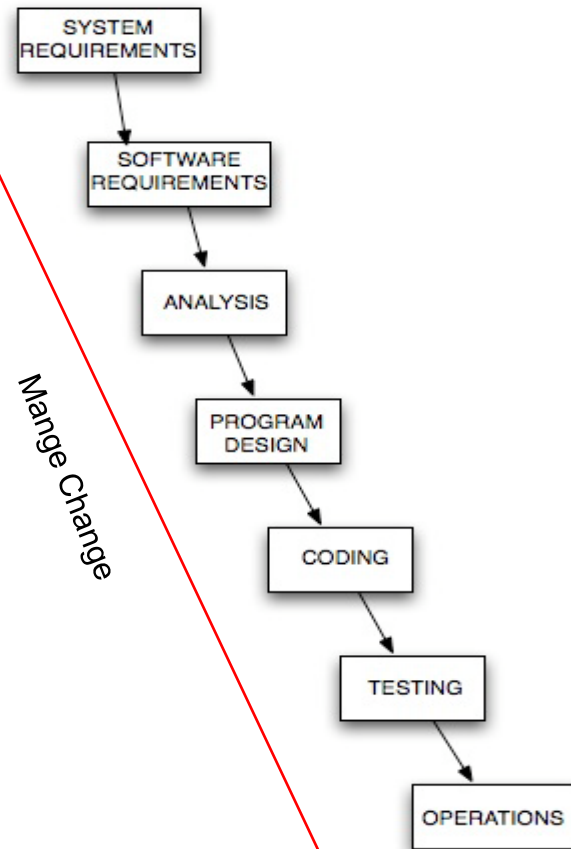
Software Development Life Cycle
Relationship between change management and SDLC

- Iterative model

    – Agile Methodology

    – Rational Unified Process (RUP)

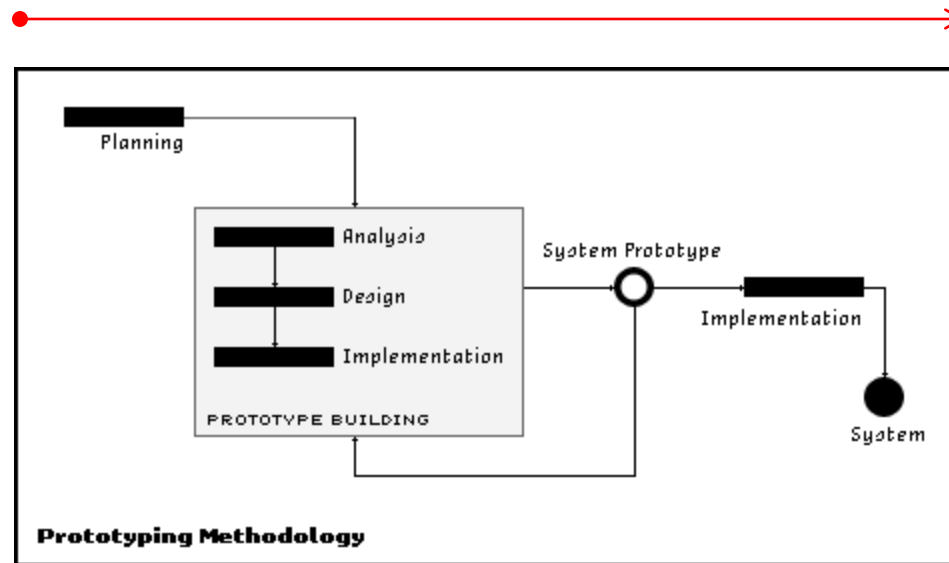   – Rapid Application Development (RAD)

    – Joint Application Development (JAD)

Software Development Life Cycle
Relationship between change management and SDLC

- Prototyping

Mange Change

Prototyping Methodology

Software Development Life Cycle
Relationship between change management and SDLC

- V Model
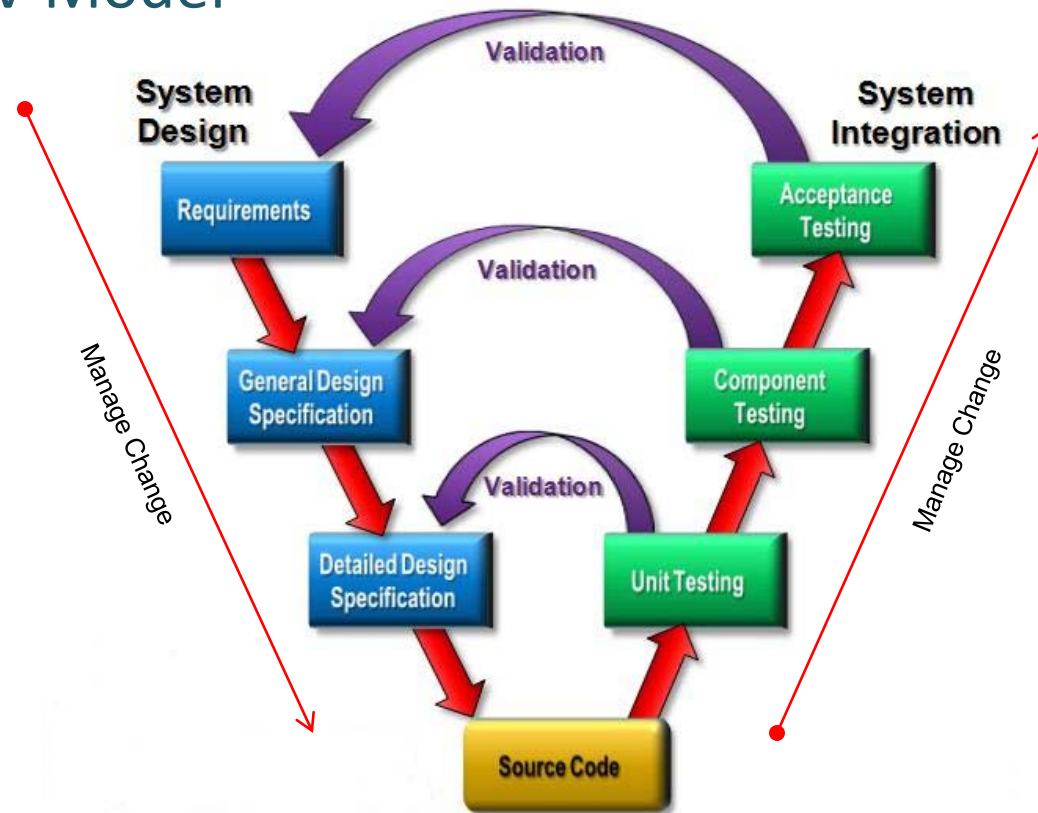
Software Development Life Cycle
Tools to better manage change

- Requirements Management

- Visual Modeling

- Automated Testing

- Change Management

Course Review

- Why change management and its significance

- Types of changes

- Change management controls

- Leading practices

- Software Development Life Cycle (SDLC)

Questions?

Contact Information

Steve Owyoung
sowyoung@kpmg.com
415-963-7603

Doug Mohrland
doug.mohrland@oracle.com
650-506-3737

Appendix I
Types of Changes

Types of changes
OS changes (Host)

- Applying OS patches
  - OS vendor recommendation
  - Opening/closing OS services
- Re-imaging
  - As a backup plan when an OS update didn't go as planned
  - As part of major/minor/emergency application changes

Types of changes
Network changes

- Software changes
  - Deploying OS
  - Patching OS

- Configuration Changes
  - Updating firewall, router, switch configuration

- Hardware changes
  - Adding/removing of network equipment

Types of changes
Application changes

- Company specific application change
  - Major, minor and emergency changes
  - New releases
  - Bug fixes
- Application configuration changes
- Database changes
  - Schema changes
  - Database upgrades (version upgrade)

Types of changes
Physical access change

- Physical access to data center
  - Preventing root level access through a system console
  - Deactivating terminated employee's physical access
  - Deactivating temporary physical access

Types of changes
Logical access change

- OS Access Change
  - privileged access to production/mission- critical server

- Application Access Change
  - privileged access to production/mission- critical application

- Network Access Change
  - privileged access to network equipment

Appendix II

Change Management Controls:

Maintain System Integrity

Change management controls

How to maintain system integrity

- Prevention
  - Restrict logical access
    - Firewall, IDS, OS and Application
  - Unnecessary services
    - Disable at the servers
    - Block by the firewalls
  - Restrict physical access
    - Restrict physical access that houses critical systems to ONLY authorized employees
    - Perform periodic physical access reviews

Change management controls

How to maintain system integrity

- Detection
  - Monitor metadata and look for changes
    - Create, store and monitor baseline metadata values
    - Metadata values: modification time, file size and cryptographic checksum
  - Integrity Management Software
    - Reads files or directories to monitor
      - critical network configuration, data files, customer database files, documents and spreadsheets
    - Takes action when a violation (change) occurs
  - Intrusion detection (IDS)

Change management controls

How to maintain system integrity

- Recovery
  - Maintain a backup copy of the production data
  - Identify changes based on the Integrity Management Software report
  - Determine whether a change is authorized or not
  - Restore a file if the change is deemed unauthorized or malicious

Appendix III
Change Management Controls: Leading Practices

Change management leading practices

Change management policy, procedure and standards

- Prioritize/categorize changes based on downtime, lead time, type of services and severity of the change (Low, Medium, High Urgent)

- Roles and responsibilities
  - Define and designate qualified personnel's roles
  - Segregation of duties (SOD)
  - Communication
  - Enforce change-management process

Change management leading practices

Change Request Management

- ## Change Request Analysis
  - Business Analysis
    - The likelihood of success
    - Significance to business
    - Resources required and business justification
  - Technical Analysis
    - System dependencies
    - Technical requirement
    - Project estimate

- ## Change Request Reporting
  - Make the change requests visible to management
  - Retain status of the change request when it is analyzed, prioritized, tested and deployed

Change management leading practices

Approval Process

- Appropriate approval should be obtained between the different phases of change management process

- Management approval should be documented

Change management leading practices

Deployment Management

- Logical environment (separate) – Development, Test/QA and Production

- Deployment process
  - High category changes
  - Low/Medium category changes
  - Emergency changes

- Leverage Technology
  - To provide auditability and versioning throughout the deployment process

Change management leading practices

Result management

- Key Performance Indicators (KPI) about the entire Change Management Process
  - Process bottlenecks, successful techniques, etc.
- Use the KPIs (by management) to make adjustments to the change management procedure and practices
- Post change implementation monitoring

Change management leading practices

Monitor application and networks

- Integrity checks
  - Automated monitoring tools
  - Incident response
  - Escalation process
- Periodic reviews
  - User access – OS, apps, network, etc.
  - System configuration – servers, network equipment, etc.