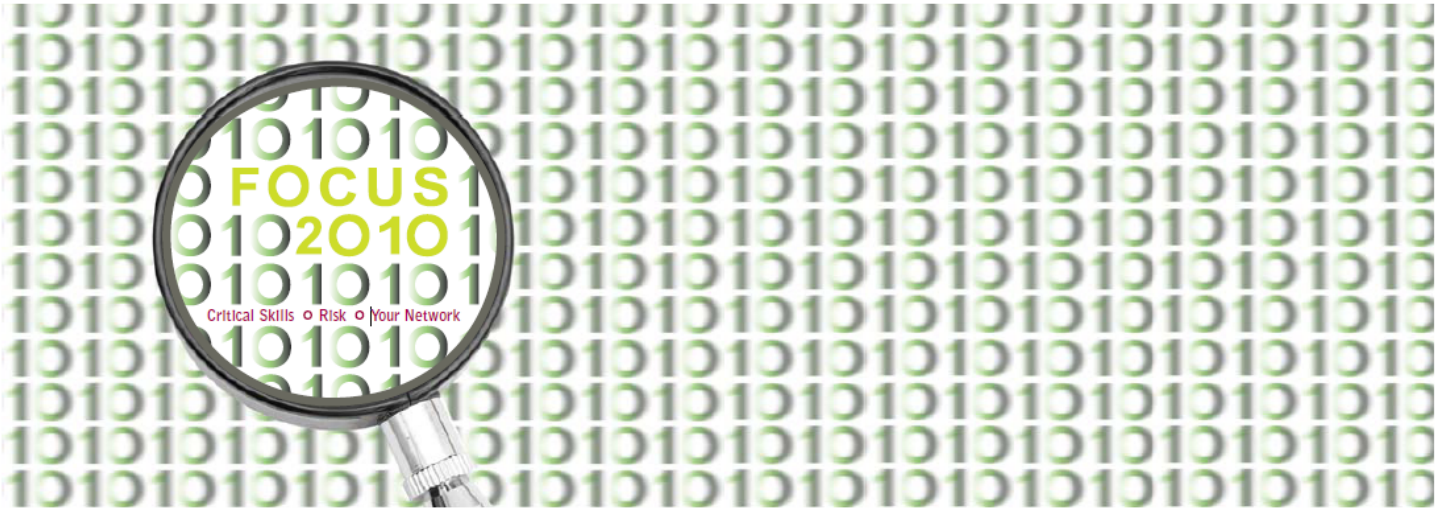
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



C21: Introduction to Change Management and SDLC

Steve Owyoung and Doug Mohrland, KPMG

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

Introduction to Change Management and SDLC

Steve Owyoung
Manager

Doug Mohrland
Manager

KPMG LLP, IT Advisory

Discussion topics

- Why change management and its significance
- Types of changes in production environment
- Change management controls
- Impact of weak change management control
- Integrity management
- Change management leading practices
- Software Development Life Cycle (SDLC)

Why change management and its significance?

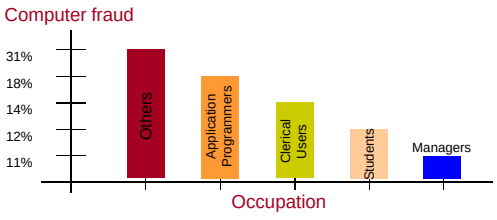
1. **Why change management and its significance?**
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

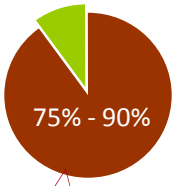
Why change management and its significance?

1. **Why change management and its significance?**
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

Total fraud losses in the United States estimated to be $994 billion in 2008

Of all the computer crimes reported:





computer crime committed by former or current employees (knowledgeable insiders)

Source: Association of Certified Fraud Examiners and National Center For Computer Crime

Why Change Management and its significance?

1. **Why change management and its significance?**
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

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

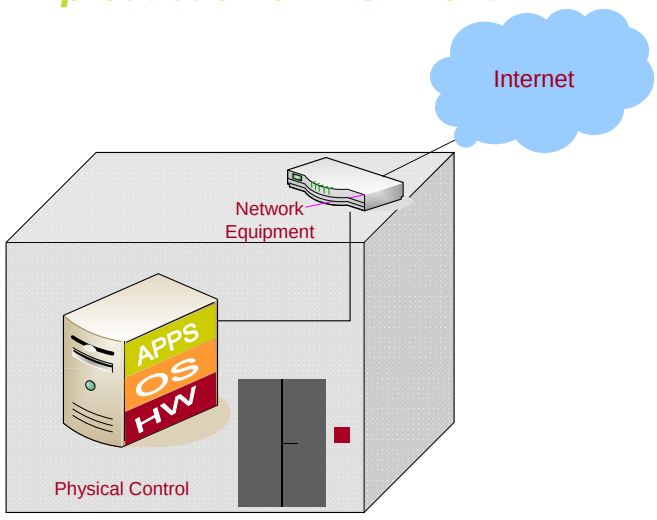
Adapting to change → Controlling change → Effecting change

FOCUS 2010

ISACA San Francisco Chapter

Types of changes
Changes in production environment

1. Why change management and its significance?
2. **Types of changes in production environment**
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle



FOCUS 2010

ISACA San Francisco Chapter

1. Why change management and its significance?
2. **Types of changes in production environment**
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

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

1. Why change management and its significance?
2. **Types of changes in production environment**
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

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

1. Why change management and its significance?
2. **Types of changes in production environment**
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

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

ISACA San Francisco Chapter

Types of changes
Physical access change

1. Why change management and its significance?
2. **Types of changes in production environment**
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

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

ISACA San Francisco Chapter

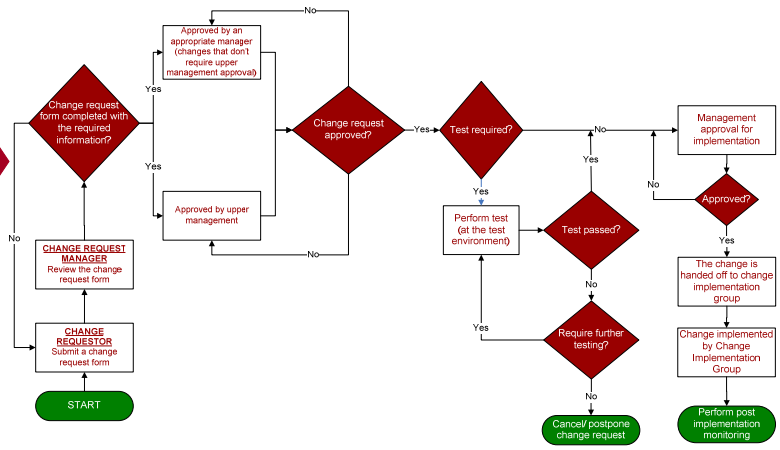
Types of changes
Logical access change

1. Why change management and its significance?
2. **Types of changes in production environment**
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

- 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

Change management controls
Planned/routing maintenance changes procedure and controls

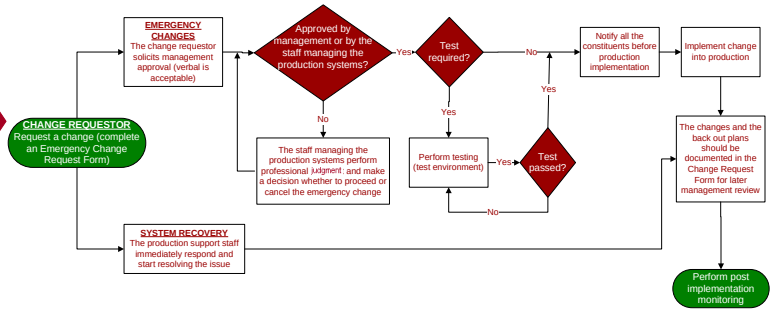
1. Why change management and its significance?
2. Types of changes in production environment
3. **Change management controls**
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle



Change management controls

Emergency/System Recovery change procedure and controls

1. Why change management and its significance?
2. Types of changes in production environment
3. **Change management controls**
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle



Impact of weak change controls

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. **Impact of weak change control**
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

Potential for **system outages**

Prone to **unplanned**, **unauthorized** and **undocumented** changes

- Unauthorized and undocumented changes
  - Causes unexplained additional problems or outages

Impact of weak change controls

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. **Impact of weak change control**
5. Integrity management
6. Change management leading practices
7. Software Development Life Cycle

- **Prone to system attack** – example denial of services
- **Misuse of resource**
  - Unplanned work
  - Creates monetary loss
- **Causes legal implication**
  - Due to the exposure of sensitive customer data
  - Due to system unavailability to customers
- **Losing a customer/ business**

ISACA San Francisco Chapter

Integrity management

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. **Integrity management**
6. Change management leading practices
7. Software Development Life Cycle

- **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

ISACA San Francisco Chapter

Integrity management

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. **Integrity management**
6. Change management leading practices
7. Software Development Life Cycle

- 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)

Integrity management

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. **Integrity management**
6. Change management leading practices
7. Software Development Life Cycle

- 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

Change management leading practices

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. **Change management leading practices**
7. Software Development Life Cycle

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

ISACA San Francisco Chapter

Change management leading practices

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. **Change management leading practices**
7. Software Development Life Cycle

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

ISACA San Francisco Chapter

Change management leading practices

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. **Change management leading practices**
7. Software Development Life Cycle

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

ISACA San Francisco Chapter

Change management leading practices

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. **Change management leading practices**
7. Software Development Life Cycle

Approval Process

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

ISACA San Francisco Chapter

Change management leading practices

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. **Change management leading practices**
7. Software Development Life Cycle

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

ISACA San Francisco Chapter

Change management leading practices

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. **Change management leading practices**
7. Software Development Life Cycle

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

ISACA San Francisco Chapter

Change management leading practices

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. **Change management leading practices**
7. Software Development Life Cycle

Monitor application and networks

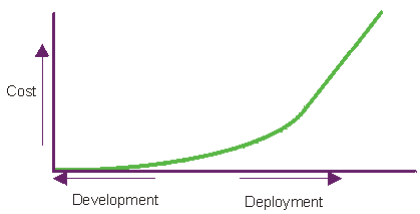
- Integrity checks
  - using automated monitoring tools
  - Incident response
    - Escalation process
- Periodic reviews
  - User access – OS, apps, network, etc.
  - System configuration – servers, network equipment, etc.

Software Development Life Cycle

Relationship between change management and SDLC

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. **Software Development Life Cycle**

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

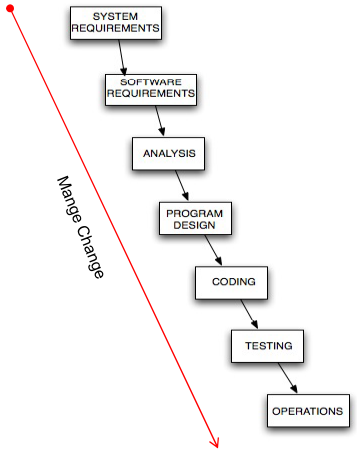


1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. **Software Development Life Cycle**

Software Development Life Cycle

Relationship between change management and SDLC

- Waterfall model



1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. **Software Development Life Cycle**

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)

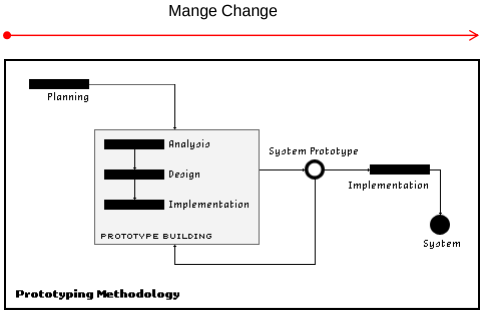
Illustration courtesy of Rational Unified Process

Software Development Life Cycle

Relationship between change management and SDLC

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. **Software Development Life Cycle**

- Prototyping

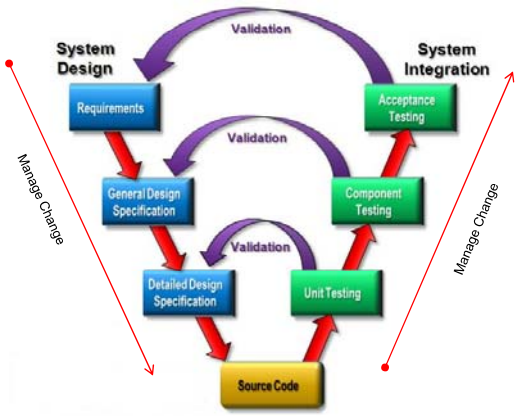


Software Development Life Cycle

Relationship between change management and SDLC

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. **Software Development Life Cycle**

- V Model



Software Development Life Cycle

Tools to better manage change

1. Why change management and its significance?
2. Types of changes in production environment
3. Change management controls
4. Impact of weak change control
5. Integrity management
6. Change management leading practices
7. **Software Development Life Cycle**

- Requirements Management
- Visual Modeling
- Automated Testing
- Change Management

ISACA San Francisco Chapter

Course Review

- Why change management and its significance
- Types of changes in production environment
- Change management controls
- Impact of weak change management control
- Integrity management
- Change management leading practices
- Software Development Life Cycle (SDLC)

ISACA San Francisco Chapter

Questions?

Contact Information

- Steve Owyoung, 415-963-7603
  sowyoung@kpmg.com
- Doug Mohrland, 415-963-7570
  dmohrland@kpmg.com