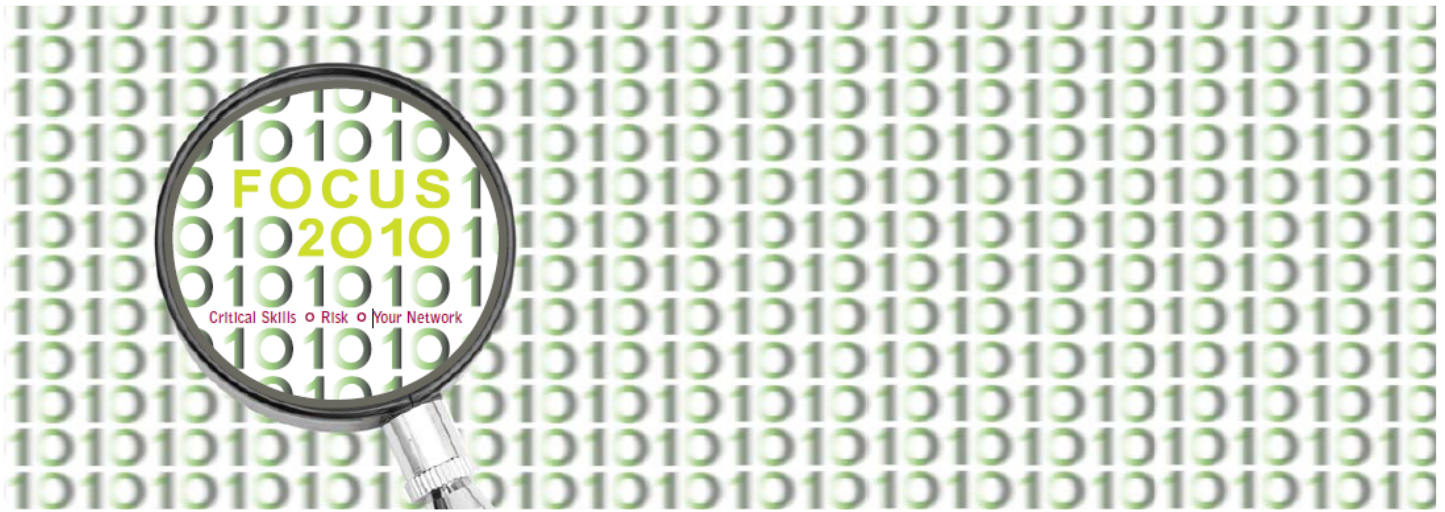


10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



## C21: Introduction to Change Management and SDLC

Steve Owyong and Doug Mohrland,  
KPMG

# Introduction to Change Management and SDLC

Steve Owyong  
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

3

## 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 fraud

Occupation

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

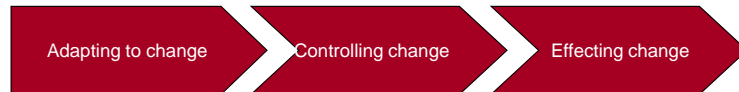
4

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

## Why Change Management and its significance?

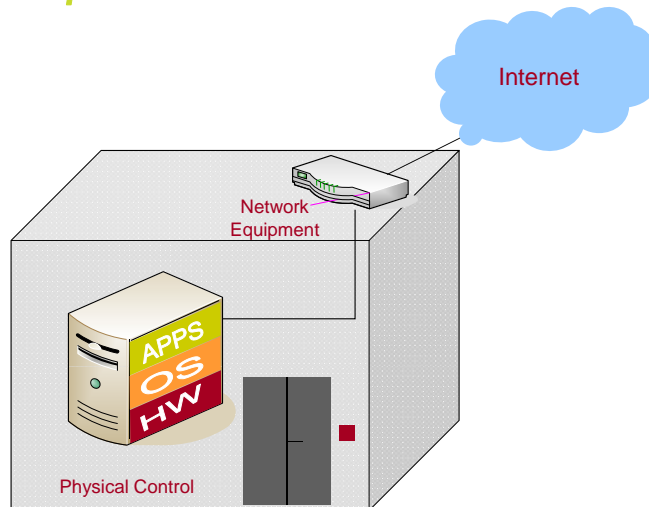
1	Why change management and its significance?
2	Types of changes in production environment
3	Change management controls
4	Impact of weak change control
5	Integrity management
6	Change management leading practices
7	Software Development Life Cycle

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



## 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



## Types of changes OS changes (Host)

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

- **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

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


- **Software changes**
  - Deploying OS
  - Patching OS
- **Configuration Changes**
  - Updating firewall, router, switch configuration
- **Hardware changes**
  - Adding/removing of network equipment


1	Why change management and its significance?
2	<b>Types of changes in production environment</b>
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

### *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)







1	Why change management and its significance?
2	<b>Types of changes in production environment</b>
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

### *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







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

### 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

FOCUS

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

## Change management controls

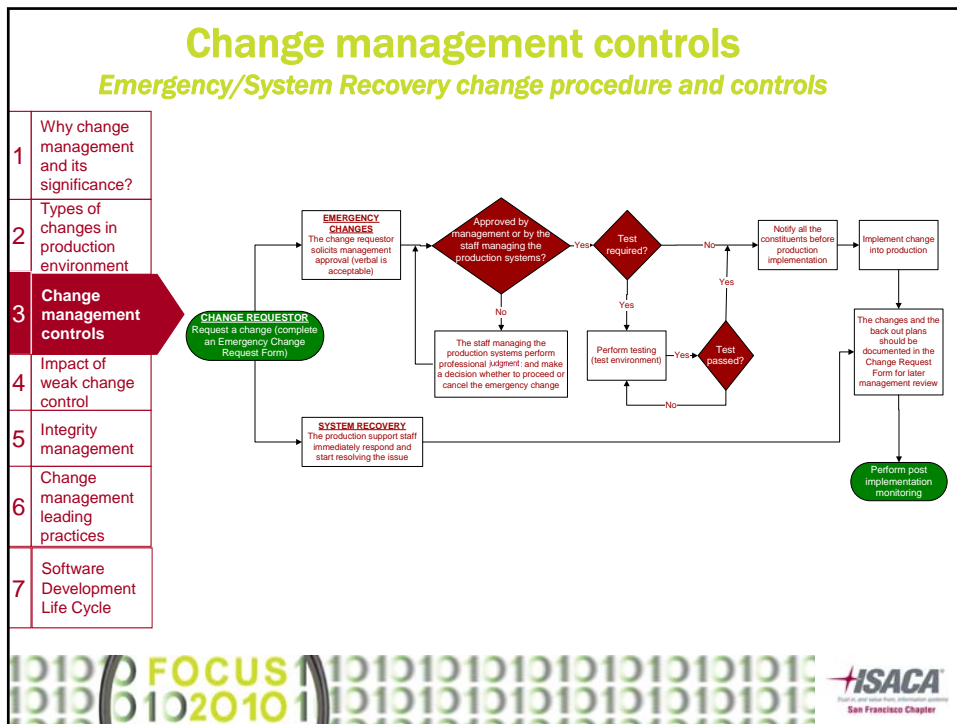
### Planned/routing maintenance changes procedure and controls

```

graph TD
    START([START]) --> CREQ[CHANGE REQUESTOR  
Submit a change request form]
    CREQ --> CM[CHANGE REQUEST MANAGER  
Review the change request form]
    CM --> D1{Change request form completed with the required information?}
    D1 -- No --> CREQ
    D1 -- Yes --> D2{Change request approved?}
    D2 -- No --> CM
    D2 -- Yes --> D3{Test required?}
    D3 -- No --> D4{Approved?}
    D4 -- No --> CM
    D4 -- Yes --> D5{Change implemented by Change Implementation Group}
    D5 --> D6{Perform post implementation monitoring}
    D6 --> END([END])
    D3 -- Yes --> D7{Perform test at the test environment}
    D7 --> D8{Test passed?}
    D8 -- No --> D9{Require further testing?}
    D9 -- No --> D4
    D9 -- Yes --> D7
    D8 -- Yes --> D4
  
```

FOCUS

ISACA  
San Francisco Chapter



## Impact of weak change controls

1	Why change management and its significance?
2	Types of changes in production environment
3	Change management controls
4	<b>Impact of weak change control</b>
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	<b>Impact of weak change control</b>
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**



## 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	<b>Integrity management</b>
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



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	<b>Integrity management</b>
6	Change management leading practices
7	Software Development Life Cycle

## Integrity management



- **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)

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	<b>Integrity management</b>
6	Change management leading practices
7	Software Development Life Cycle

## Integrity management

- **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	<b>Change management leading practices</b>
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



## 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	<b>Change management leading practices</b>
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



## 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	<b>Change management leading practices</b>
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



## 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	<b>Change management leading practices</b>
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



## 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	<b>Change management leading practices</b>
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



## 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	<b>Change management leading practices</b>
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



## 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	<b>Change management leading practices</b>
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.

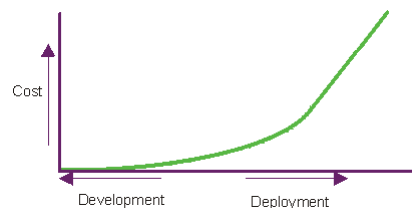


## Software Development Life Cycle

### 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	<b>Software Development Life Cycle</b>

- 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



## 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	<b>Software Development Life Cycle</b>

○ Waterfall model

```

graph TD
    SR[SYSTEM REQUIREMENTS] --> SWR[SOFTWARE REQUIREMENTS]
    SWR --> A[ANALYSIS]
    A --> PD[PROGRAM DESIGN]
    PD --> C[CODING]
    C --> T[TESTING]
    T --> O[OPERATIONS]

```

FOCUS

INSTITUTE OF INFORMATION SYSTEMS AUDITING AND CERTIFICATION  
San Francisco Chapter

## 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	<b>Software Development Life Cycle</b>

○ Iterative model

- Agile Methodology
- Rational Unified Process (RUP)
- Rapid Application Development (RAD)
- Joint Application Development (JAD)

```

graph TD
    IP[Initial Planning] --> BM[Business Modeling]
    BM --> R[Requirements]
    R --> AD[Analysis & Design]
    AD --> I[Implementation]
    I --> T[Test]
    T --> D[Deployment]
    D --> E[Evaluation]
    E --> ENV[Environment]
    ENV --> IP
    CCM((Config. & Change Management)) --- R
    CCM --- AD
    CCM --- I
    CCM --- T
    CCM --- E
    CCM --- ENV

```

FOCUS

INSTITUTE OF INFORMATION SYSTEMS AUDITING AND CERTIFICATION  
San Francisco Chapter

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

The diagram illustrates the Prototyping Methodology. It starts with 'Planning', followed by 'Analysis', 'Design', and 'Implementation' within a box labeled 'PROTOTYPE BUILDING'. A 'System Prototype' is created, leading to 'Implementation' and finally 'System'. A red arrow labeled 'Manage Change' points from the 'System' back to the 'Planning' stage, indicating a feedback loop.

**Prototyping Methodology**

# 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

The diagram illustrates the V Model. The left side of the 'V' represents the development phases: 'System Design' (Requirements, General Design Specification, Detailed Design Specification) leading down to 'Source Code'. The right side represents the testing phases: 'Unit Testing', 'Component Testing', and 'Acceptance Testing' leading up to 'System Integration'. Purple curved arrows labeled 'Validation' connect the development phases to their corresponding testing phases. Red arrows labeled 'Manage Change' point from the 'System Integration' stage back to the 'System Design' stage, indicating a feedback loop.

# 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



## 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)



## Questions?



## Contact Information

- Steve Owyong, 415-963-7603  
[sowyoung@kpmg.com](mailto:sowyoung@kpmg.com)
- Doug Mohrland, 415-963-7570  
[dmohrland@kpmg.com](mailto:dmohrland@kpmg.com)

