Introduction to Change Management and SDLC

Steve Owyoung
Sr. Manager
KPMG LLP, IT Advisory

Doug Mohrland
Audit Manager
Oracle Corporation
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?

- Types of changes in production environment
- Change management controls
- Impact of weak change control
- Integrity management
- Change management leading practices
- Software Development Life Cycle

Constant Environment Change

- Customer demand/need
- Government
- Competition
- Technology

Back to Business
Why change management and its significance?

Total fraud losses in the United States estimated to be $994 billion in 2008.
Of all the computer crimes reported:

- Computer fraud
  - 31% Others
  - 18% Application Programmers
  - 14% Clerical Users
  - 12% Students
  - 11% Manager

75% - 90% computer crime committed by former or current employees (knowledgeable insiders)
Why Change Management and its significance?

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

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

Adapting to change  
Controlling change  
Effecting change
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

Internet

Network Equipment

Physical Control

APPs

OS

HW

Back to Business
Change management controls

**Planned/routine maintenance changes procedure and controls**

1. **Why change management and its significance?**
   - Change request form completed with the required information?
     - Yes
       - Change request approved?
         - Yes
           - Test required?
             - Yes
               - Manage test approval
             - No
               - Perform test (at the test environment)
             - Yes
               - Test passed?
                 - Yes
                   - Approved?
                     - Yes
                       - Management approval for implementation
                     - No
                       - The change is handed off to change implementation group
                 - No
                   - Require further testing?
                     - Yes
                       - Change implemented by Change Implementation Group
                     - No
                       - Perform post implementation monitoring
                 - No
                   - Cancel/postpone change request
     - No
       - Approved by upper management

2. **Types of changes in production environment**
   - Change request approved?
     - Yes
       - Test required?
         - Yes
           - Perform test (at the test environment)
         - No
           - Test passed?
             - Yes
               - Approved?
                 - Yes
                   - Management approval for implementation
                 - No
                   - The change is handed off to change implementation group
             - No
               - Require further testing?
                 - Yes
                   - Change implemented by Change Implementation Group
                 - No
                   - Perform post implementation monitoring
     - No
       - Approved by upper management

3. **Change management controls**
   - Change request form completed with the required information?
     - Yes
       - Change request approved?
         - Yes
         - Test required?
           - Yes
             - Perform test (at the test environment)
           - No
             - Test passed?
               - Yes
                 - Approved?
                   - Yes
                     - Management approval for implementation
                   - No
                     - The change is handed off to change implementation group
               - No
                 - Require further testing?
                   - Yes
                     - Change implemented by Change Implementation Group
                   - No
                     - Perform post implementation monitoring
         - No
       - Approved by upper management

4. **Impact of weak change control**
   - Change request approved?
     - Yes
       - Test required?
         - Yes
           - Perform test (at the test environment)
         - No
           - Test passed?
             - Yes
               - Approved?
                 - Yes
                   - Management approval for implementation
                 - No
                   - The change is handed off to change implementation group
             - No
               - Require further testing?
                 - Yes
                   - Change implemented by Change Implementation Group
                 - No
                   - Perform post implementation monitoring
     - No
       - Approved by upper management

5. **Integrity management**
   - Change request approved?
     - Yes
       - Test required?
         - Yes
           - Perform test (at the test environment)
         - No
           - Test passed?
             - Yes
               - Approved?
                 - Yes
                   - Management approval for implementation
                 - No
                   - The change is handed off to change implementation group
             - No
               - Require further testing?
                 - Yes
                   - Change implemented by Change Implementation Group
                 - No
                   - Perform post implementation monitoring
     - No
       - Approved by upper management

6. **Change management leading practices**
   - Change request approved?
     - Yes
       - Test required?
         - Yes
           - Perform test (at the test environment)
         - No
           - Test passed?
             - Yes
               - Approved?
                 - Yes
                   - Management approval for implementation
                 - No
                   - The change is handed off to change implementation group
             - No
               - Require further testing?
                 - Yes
                   - Change implemented by Change Implementation Group
                 - No
                   - Perform post implementation monitoring
     - No
       - Approved by upper management

7. **Software Development Life Cycle**
   - Change request approved?
     - Yes
       - Test required?
         - Yes
           - Perform test (at the test environment)
         - No
           - Test passed?
             - Yes
               - Approved?
                 - Yes
                   - Management approval for implementation
                 - No
                   - The change is handed off to change implementation group
             - No
               - Require further testing?
                 - Yes
                   - Change implemented by Change Implementation Group
                 - No
                   - Perform post implementation monitoring
     - No
       - Approved by upper management
**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**

   - **Emergency Changes**
     - The change requestor solicits management approval (verbal is acceptable)

   - **System Recovery**
     - The production support staff immediately respond and start resolving the issue

4. **Impact of weak change control**

5. **Integrity management**

6. **Change management leading practices**

7. **Software Development Life Cycle**

Back to Business
# 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

### Impact of weak change controls:

- **Financial loss**
  - Brand/reputational damage
  - Losing a customer/ business

- **Legal exposure** (sensitive data disclosure)

- Unplanned, unauthorized and undocumented changes
- Prone to system attack / outages (DoS)
- Misuse of resources (unplanned work)
# Integrity management

- **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

## Why change management and its significance?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Why change management and its significance?</td>
</tr>
<tr>
<td>2</td>
<td>Types of changes in production environment</td>
</tr>
<tr>
<td>3</td>
<td>Change management controls</td>
</tr>
<tr>
<td>4</td>
<td>Impact of weak change control</td>
</tr>
<tr>
<td>5</td>
<td>Integrity management</td>
</tr>
<tr>
<td>6</td>
<td>Change management leading practices</td>
</tr>
<tr>
<td>7</td>
<td>Software Development Life Cycle</td>
</tr>
</tbody>
</table>

**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
# 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)

<table>
<thead>
<tr>
<th></th>
<th>Why change management and its significance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Types of changes in production environment</td>
</tr>
<tr>
<td>3</td>
<td>Change management controls</td>
</tr>
<tr>
<td>4</td>
<td>Impact of weak change control</td>
</tr>
</tbody>
</table>

### Integrity management

- Change management leading practices
- Software Development Life Cycle

---

**Back to Business**
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

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

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

<table>
<thead>
<tr>
<th></th>
<th>Why change management and its significance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

### 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 controls
- Segregation of duties (SOD)
- Communication
- Integrity management

### Integrity management

### Software Development Life Cycle

### Change management leading practices

### Software Development Life Cycle
### Change management leading practices

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

#### 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

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

**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

<table>
<thead>
<tr>
<th></th>
<th>Why change management and its significance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Types of changes in production environment</td>
</tr>
<tr>
<td>3</td>
<td>Change management controls</td>
</tr>
<tr>
<td>4</td>
<td>Impact of weak change control</td>
</tr>
<tr>
<td>5</td>
<td>Integrity management</td>
</tr>
<tr>
<td>6</td>
<td>Change management leading practices</td>
</tr>
<tr>
<td>7</td>
<td>Software Development Life Cycle</td>
</tr>
</tbody>
</table>
# Change management leading practices

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

## 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

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

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**

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

- 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

![Cost vs. Development and Deployment graph](image)
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

- Waterfall model

Back to Business
Software Development Life Cycle

Relationship between change management and SDLC

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

- **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

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

Prototyping Methodology

Mange Change

Planning

Analysis

Design

Implementation

System Prototype

System

Implementation
Software Development Life Cycle

Relationship between change management and SDLC

- V 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

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 Owyoung  
 sowyoung@kpmg.com  
 415-963-7603

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

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

1. Why change management and its significance?

2. Types of changes in production environment
   - Change management controls
   - Impact of weak change control
   - Integrity management
   - Change management leading practices

3. Software changes
   - Deploying OS
   - Patching OS

4. Configuration Changes
   - Updating firewall, router, switch configuration

5. Hardware changes
   - Adding/removing of network equipment
## Types of changes

### Application changes

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Why change management and its significance?</td>
</tr>
<tr>
<td>2</td>
<td>Types of changes in production environment</td>
</tr>
<tr>
<td>3</td>
<td>Change management controls</td>
</tr>
<tr>
<td>4</td>
<td>Impact of weak change control</td>
</tr>
<tr>
<td>5</td>
<td>Integrity management</td>
</tr>
<tr>
<td>6</td>
<td>Change management leading practices</td>
</tr>
<tr>
<td>7</td>
<td>Software Development Life Cycle</td>
</tr>
</tbody>
</table>

- **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

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

- **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