Agenda

- PCI Assessment
- Auditor’s Role in System Development
- BYOD

Agenda

- The Need / The Risks
- Audit Basics
- Types of Reviews
- Advisory Services
- Reporting
## System Development Life Cycle

<table>
<thead>
<tr>
<th>Methodology</th>
<th>Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Helps ensure that the development of an application or system occurs in a formal and controlled manner</td>
<td>• Provides a method for implementing controls during the development of the system, rather than retrofitting the system with necessary controls after it is in production environment</td>
</tr>
</tbody>
</table>

---

## SDLC - Definition

The system development life cycle (or Solution Delivery Methodology – SDM) is the process:

1. Involving multiple stages (feasibility to carrying out post implementation)
2. Used to convert a management need into an application system
3. Which is custom-developed or purchased or a combination of both
Risk Definition

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Areas of Focus

• Governance:
  • Business & IT Alignment
  • Project Management
  • Organizational Change Management

• Tactical
  • IT Solution Readiness
  • Post Implementation

Diagram:
- Business & IT Alignment
- Project Management
- IT Solution Readiness
- Post Implementation
- Organizational Change Management

Page 5

Page 6
High Level Risks

Market
- Disruption of service
- Competitive advantage
- Brand image

Financial
- Loss of revenue
- Loss of ROI
- Loss of shareholders / investors
- Regulatory compliance fines

Technology
- Facility closure
- Facility damage
- System unavailable

People
- Loss of business experts
- Loss of IT people
- Inexperienced people

Why Audit IT Projects?

Businesses invest heavily in IT Projects to:

- Enable business process efficiencies in order to save money
- Automate key processes and controls
- Manage risk
- Meet regulatory and legal requirements
- Enable new business models and allow the company to enter new markets
- Many other reasons...
Why Audit IT Projects?

- Identification of key risks early on in the project
- Adds value by evaluating the effectiveness of risk management on both IT and Organizational aspects
- Offers an independent assessment on whether the project has reached stated objectives

Business & IT Alignment

Business Strategy

IT Strategy

Alignment is maintained throughout the project

The vision & objectives of both IT and the business are understood and in harmony

Project is in line with strategy of the company
Audit Charter Should.....

- Specify the Internal Auditor is permitted to be involved in, and comment on, the development of application systems

- State the Internal Auditor should report all concerns about the viability of the project to the Project Sponsor and, if necessary, Senior Management
The Players

- Financial Audit
- IT Audit
- Operations Audit
- Government Audit

Auditor’s Strengths

- Internal control expertise
- Knowledge of the processes
- Knowledge of the organization
- Objective perspective and independence
- Past work experience in other organizations
- Current control environment (SOC-1, SOC-2, Sox / MAR, YE Financials)
- Knowledge of individuals and their responsibilities
### Competencies

- Management concepts
- Auditing concepts
- Negotiating skills
- Communication skills
- Audit tools (CAATs)
- Sense of humor

### Independence

The auditor, while reporting to the CAE, should be independent of the project team responsible for designing or acquiring and implementing the application system.
Independence – The IIA

1100 Independence and Objectivity

- The internal audit activity must be independent, and internal auditors must be objective in performing their work.

1110 – Organizational Independence

- The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities.
- The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.
- The internal audit activity should be free from interference in determining the scope of internal auditing, performing work, and communicating results.

Management’s Role

Advise the CAE of the following:

- Updates or changes to systems
- Updates or changes to policies and procedures
- Changes in organizational structure
- Changes to major strategies and objectives
- Significant defalcations, system failures and operational losses


Agenda

- Audit Basics
- The Need / The Risks
- Types of Engagements
- Advisory Services
- Reporting

Types of Project Engagements

- Methodology Assessment
- Project Risk Assessment
- Readiness Assessment
- Key Phase Review
- Post-Implementation Review
- Advisory Services
Methodology Assessment

Why
Determine if methodology exists, is complete and meets the needs of the organization

When
Anytime, preferably before any detailed project reviews are conducted

How
Coordinate with PMO, research PM best practices, review history of PM problems

Methodology Assessment

Presence of a formal process

Process documentation – approved and endorsed by senior IT leadership

Project Plan

Mandatory sign-offs at each stage gate

Required “go / no-go” decision points

Standard templates and forms

Standard naming conventions

Escalation processes
Methodology Assessment

Exception protocols

Formalized testing methods

Source Control

Peer Review

Change control process

Standard project management templates / reports

Test environment separate from production

Formal reporting processes / templates

Consistent use of metrics (red, yellow, green)

Stakeholder involvement and engagement (legal, security, finance, audit, etc.)

Issue and Action logs

Quality Review Board / Function

Defined Documents: Requirements, Design, Testing, etc.

Centralized place for storing documents
Methodology Assessment

- Exists, is adhered to and is used by all projects
- Provides flexibility to support project sizes and types
- Provides sufficient structure to help PMs and reduce the risk of project failure
- Is based on best practices
  - PM: PMBOK, PRINCE2, etc.
  - Technical: SDLCs, SEI, etc.
  - Regulatory and Legal as required

Auditors should ensure the methodology

Project Risk Assessment

- Why: Assess any potential risk areas
- When: Anytime during project execution
- How: Identify key risks that could affect the project and how they are tracked and monitored
**What to Look For**

- Executive management support and ownership
- User involvement
- Clear statement of requirements
- Proper planning
- Realistic expectations
- Hardworking, focused and competent staff
- Clear visions and objectives

**Pre-Launch Readiness Assessment**

**Why**
Determine readiness for final go-live

**When**
Pre-launch

**How**
Ensure required actions are complete: business approvals, testing, documentation, etc.
What to Look For

- All testing completed
- Parallel processing completed
- Documentation updated
- Staff trained
- Help Desk trained
- Communication plan deployed

Key Phase Review

**Why**
Ensure a project phase was completed as expected and in accordance with the PM processes

**When**
Before or during high-risk phases

**How**
Review against (a) stated objectives and requirements; (b) methodology adherence; (c) benefits realization

Benefits Realization ????
Post-Implementation Review

**Why**
Ensure project accomplished what was expected

**When**
After go-live and system is stable but before project team disbands

**How**
Review against stated objectives and requirements; or methodology adherence; or benefits realization

---

What to Look For

- New processes are followed
- Users understand the system & functionality
- Resistance to change - people finding workarounds
- Allow adequate stabilization period

**ISSUE**

Too late and costly to fix things easily
Advisory Services

**Why**
Ensure proper controls, security, audit trails, etc. are included

**When**
During all key phases of the project

**How**
Being involved with project, reviewing requirements, etc.

### Agenda

- Audit Basics
- The Need / The Risks
- Types of Engagements
- Advisory Services
- Reporting
**Why Be Involved?**

The utilization and reliance upon technology to manage and support the business has increased exponentially over the last two decades. Companies continue to invest in technology to reduce admin costs, increase efficiencies and achieve competitive advantages. IT Auditing has evolved into a necessary requirement to manage and govern an organization’s risk and compliance posture. Proactive controls consulting will result in appropriate controls being implemented early in the development process.

---

**Corporate Executive Board**

**Project Management is an audit area of concern**

Financial Loss: late projects change cost-benefits, and could harm company's reputation

Failed business expansion: implementation failures may impact income revenue stream and affect business partners / customers

Inadequate IT controls: technology upgrades are expensive and can have adverse affects if not implemented properly

Misaligned strategy: projects not aligned with corporate strategy may not add expected value

Repeated mistakes: failure to analyze completed projects cannot rectify process inefficiencies in future projects
### Project Factoids

**More than 60% of Large Projects**
- fail to meet business objectives
- are significantly late
- are severely over budget

**Success rates of execution**
- 50% are over budget
- 58% missed major milestones
- 42% had defects after production

---

### Corporate Executive Board

**After Implementation**
- $32,000 - annual cost of remediating one audit issue discovered after implementation
- $4,700,000 - annual cost of remediating all audit issues discovered after implementation

**Before Implementation**
- $4,000 - average cost of embedding a control during development
- $562,000 - average cost of embedding controls during development

Which column do you want to be in?
SDLC Risks

Adoption of inappropriate SDLC for the application
Inadequate controls in the SDLC process
Inappropriate technology and architecture
Scope variations

User requirements and objectives not met by the application
Lack of management support
Time and cost over-runs
Inadequate quality of the application

Inadequate project management
Inadequate stakeholder (including internal audit) involvement
Insufficient attention to security and controls in the application
Inadequate testing

SDLC Risks

Performance criteria not being met
Inappropriate resourcing / staffing model
Insufficient attention to other dependencies
Inadequate configuration management

Inadequate staffing skills
Insufficient documentation
Poor planning for data conversion and cutover
Post cut-over disruption to business

Inadequate contractual protection
Inadequate adherence to chosen SDLC
Inadequate training
No disaster recovery process
Project Success Factors

1. User Involvement: Business and IT users are involved with key consensus-building, decision-making, and information-gathering processes.

2. Executive Support: Key executives provide alignment with business strategy, as well as financial, emotional, and conflict resolution support.

3. Clear Business Objectives: Stakeholders understand the core value of the project and how it aligns with business strategy.

4. Agile Optimization: Project uses iterative development and optimization processes to avoid unnecessary features and ensure critical features are included.

5. Emotional Maturity: Project manager directs the emotions and actions of project stakeholders and avoids ambition, arrogance, ignorance, abstinence, and fraudulence.

6. Project Management Expertise: Organization uses project managers who understand the basic skills and practices, such as certified PM Professional from the Project Management Institute.

7. Financial Management: Project manager is able to manage financial resources, account for project budget/costs, and demonstrate the value of the project.

8. Skilled Resources: Skilled project personnel are acquired, managed, retained, and controlled to move forward in the face of turnover and other personnel hurdles.

9. Formal Methodology: There is a predefined set of process-based techniques that provide a road map on when, how, and what events should occur in what order.

10. Tools and Infrastructure: The project infrastructure is built and managed with tools that enable management of tasks, resources, requirements, change, risks, vendors, user acceptance, and quality management.
Audit Department

Audit Fantasy
• Unlimited staff
• Unlimited hours
• Unlimited budget

Audit Reality
• Limited staff
• Limited hours
• Limited budget

Selection of Engagements

Conduct a risk analysis to identify projects or initiatives that present the greatest risk using enterprise resources:
### Risk Analysis Template

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Factors</th>
<th>Response</th>
<th>Risk</th>
<th>Score</th>
<th>Comment/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Risk</td>
<td>Business Owner</td>
<td>MEDIUM</td>
<td>75</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Risk</td>
<td>PM Lead</td>
<td>LOW</td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Risk</td>
<td>mandated by Law, Contract, Company etc. (if yes please indicate mandate origin in comment section)</td>
<td>N/A</td>
<td>HIGH</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Business Risk</td>
<td>Other Project Dependencies</td>
<td></td>
<td>HIGH</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Technical Risk</td>
<td>Data Complexity</td>
<td></td>
<td>N/A</td>
<td>HIGH</td>
<td>75</td>
</tr>
<tr>
<td>Regulatory Risk</td>
<td>Data Type</td>
<td>Medium Sensitivity</td>
<td>MEDIUM</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Technical Risk</td>
<td>Data Transmittal/Access Method</td>
<td>New Method of Transmittal or Remote Access</td>
<td>MEDIUM</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Project Risk</td>
<td>Estimated Project Duration</td>
<td>1-6 months</td>
<td>HIGH</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Business Risk</td>
<td>Estimated Project Duration</td>
<td>$1,000,000 - $10,000,000</td>
<td>MEDIUM</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Business Risk</td>
<td>Corporate Priority</td>
<td>Remote/Indirect</td>
<td>HIGH</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Technical Risk</td>
<td>Technology Used</td>
<td>mix of new and current</td>
<td>MEDIUM</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Technical Risk</td>
<td>T Impact</td>
<td>Severe or not considered</td>
<td>HIGH</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Business Risk</td>
<td>Results Subject to External Audit</td>
<td>Yes</td>
<td>HIGH</td>
<td>75</td>
<td></td>
</tr>
</tbody>
</table>

#### Risk Rating per Risk Category

<table>
<thead>
<tr>
<th>Business Risk (300)</th>
<th>275</th>
<th>Low Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Risk (300)</td>
<td>225</td>
<td>Medium Risk</td>
</tr>
<tr>
<td>Regulatory Risk (225)</td>
<td>300</td>
<td>High Medium</td>
</tr>
<tr>
<td>Technical Risk (450)</td>
<td>400</td>
<td>High Risk</td>
</tr>
</tbody>
</table>

#### Total Risk Score

1100

Page 47

---

### Provides Summary

<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Nantional Provider Identifier (NPI)</td>
<td>1368.75</td>
</tr>
<tr>
<td>2 BHI</td>
<td>1318.75</td>
</tr>
<tr>
<td>3 Enterprise Content Management</td>
<td>1246.75</td>
</tr>
<tr>
<td>4 Enterprise Operational Data Store</td>
<td>1246.25</td>
</tr>
<tr>
<td>5 Distributed Environment Access Clean-Up</td>
<td>1093.65</td>
</tr>
<tr>
<td>6 Workers Choice Conversion</td>
<td>1017.5</td>
</tr>
<tr>
<td>7 Manager of Managers</td>
<td>1121.25</td>
</tr>
<tr>
<td>8 Enterprise Search Capability</td>
<td>1098.75</td>
</tr>
<tr>
<td>9 PeopleSoft v8.9 Upgrade</td>
<td>987.5</td>
</tr>
<tr>
<td>10 ABS</td>
<td>950</td>
</tr>
<tr>
<td>11 Re-engineer Shared Claims Processing</td>
<td>948.75</td>
</tr>
<tr>
<td>12 Application Optimization</td>
<td>887.5</td>
</tr>
<tr>
<td>13 Off Plan Development</td>
<td>826.23</td>
</tr>
<tr>
<td>14 Provider Data Accuracy</td>
<td>847.3</td>
</tr>
<tr>
<td>15 Enterprise IPR</td>
<td>825</td>
</tr>
<tr>
<td>16 HRT - RHIO Initiatives - Participation &amp; Leadership</td>
<td>815</td>
</tr>
<tr>
<td>17 Unique BIN/PCN</td>
<td>812.5</td>
</tr>
<tr>
<td>18 Offsite Encryption Phase I</td>
<td>812.5</td>
</tr>
<tr>
<td>19 FCR</td>
<td>809.25</td>
</tr>
<tr>
<td>20 ITG - In Center Datat Replication</td>
<td>807.5</td>
</tr>
<tr>
<td>21 EMC Net Replacement</td>
<td>773.75</td>
</tr>
<tr>
<td>22 BlueCap</td>
<td>774.25</td>
</tr>
</tbody>
</table>

Average Risk Score: 967.27
Average Risk Rating: Medium

Page 48
Advisory Engagement Lifecycle

Similar to the audit process, a standard process and methodology is executed

---

Getting Started

- Project Executive and Project Manager
  - Meet With

- Ask “What keeps you awake at night”?
  - Explain the Services

- “tell me where the issues are and I’ll find them”
  - Act Like a Confessor

- What is in scope
  - Agree on

- What is not in scope
  - No Charge

- Stress that the services are free – time will not be charged to the project
  - Establish

- Report protocols
- Frequency
Getting Started

- Do they all know the big picture
- Do they understand their roles
- Do they work well together
- How is morale

Talk to the project team:

- The history of the project especially the budget
- The local languages / jargon

Understand

- Members of audit: financial / operational / government, as needed

Learn

- CobiT

Involve others

Use

CobiT

Control Objectives for Information and Related Technologies

An international unifying framework that integrates all of the main global IT standards, including ITIL, CMMI and ISO 17799

A product of 15 years of research and cooperation among global IT and business experts

A tool for compliance with Sarbanes-Oxley and many other global standards
CobiT and SOX / MAR

The PCAOB standards:
• specific requirements for auditors to understand the flow of transactions
• how transactions are initiated, authorized, recorded, processed and reported

Define the IT systems involved in financial reporting and are considered in the design and evaluation of internal controls

CobiT

Defines seven criteria to be met by systems:
- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

Evaluate how effectively the SDLC processes contribute towards the adequate fulfillment of these criteria.
## CobiT Domains

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

## CobiT

### Plan and Organize
- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- **PO10 Manage Projects**

### Acquire and Implement
- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources
- AI6 Manage Changes
- AI7 Install and Accredit Solutions and Changes
# Managing Projects

## Control Objective

**PO 10.1 Program Management Framework**

Maintain the program of projects, related to the portfolio of IT-enabled Investment program's objectives. Coordinate the activities and interdependencies of multiple projects, manage the contribution of all the Projects with the program to expected outcomes, and resolve resource Requirements and conflicts.

## Control Activities

1. Define and document the program, including all projects required to achieve the program's expected business outcomes. Specify required resources, including funding, project managers, project teams, IT resources and business resources where applicable. Gain formal approval of the document from key business and IT stakeholders.
2. Assign accountability clearly and unambiguously for each project, including achieving the benefits, controlling the costs, managing the risks and coordinating the project activities.
3. Determine the interdependencies of multiple projects in the program, and develop a schedule for their completion that will enable the overall program schedule to be met.
4. Determine program stakeholders inside and outside the enterprise, and establish and maintain appropriate levels of coordination, communication and liaison with these parties.
5. Verify periodically with the business that the current program as designed will meet business requirements and make adjustments as necessary. Review progress of individual projects and adjust the availability of resources as necessary to meet schedule milestones.
Buy versus Build

Development effort may be done in house OR Purchased Software Solution OR Both

Buy versus Build - CobiT

High-level control objectives with reference to acquisition of application systems:

- Automated Solutions (AI1)
- Acquire and Maintain Application Software (AI2)

High-level control objectives regarding:

- Manage Projects (PO10)
- Manage Quality (PO11)
- Ensure System Security (DS5)
SDLC Phases

- Initiation & Planning
- Requirements and Analysis
- Logical Design
- Physical Design
- Unit Testing
- System / User Acceptance Testing
- Production Prep
- Install / Post Install

Where do we spend our time?

Author’s Time Allocation by Phase

- Initiation & Planning, 5%
- Requirements and Analysis, 20%
- Logical Design, 10%
- Physical Design, 5%
- Unit Testing, 10%
- Production Prep, 10%
- Install / Post Install, 5%
- System / User Acceptance Testing, 35%
Auditor’s Concern by Risk

Areas of Concern

Project Management

- Project aligned with corporate strategy to add expected value
- Oversight process
- Risk / issue / cost management
- Planning / dependency review
- Stakeholder involvement
- Key deliverables by phase
- Project schedule updates
- Scope control – change management process
- Managing contractors
Quick Test

Are we embedded in team?
Is it a full time job?
Do we report to the Project Lead?
Do we report our time to the project?
Do we "design" control solutions?
Do we give control guidance?
Do we do our own testing?
Do we attend all meetings?

Quick Test

Do we sign-off at critical phases?
Do we provide feedback to the Executive Sponsors
Do we provide status reports?
Are we on the Executive Steering Committee?
Do we create a controls inventory?
## Controls Inventory

<table>
<thead>
<tr>
<th>Control Name</th>
<th>Control Objective</th>
<th>Source of Control</th>
<th>Control Activity</th>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
<th>Testing Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3000X</td>
<td>3000X</td>
<td>3000X</td>
<td>3000X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SDLC Phases

- **Initiation**
- **Requirements**
- **Logical Design**
- **Physical Design**
- **Unit Testing**
- **System / User Testing**
- **Production Preparation**
- **Installation**
Project Initiation

- Cost / benefits are reasonable and verifiable
- Alternative solutions / vendors considered
- Deliverables
  - Project objectives
  - Project scope, benefits and approach
  - Project assumptions and constraints
  - Completed / approved Business Case or Demand Management

Business Case Review

Key components of the business case should include:

- Benefits that are realistic, understood, and measurable
- Environmental concerns such as the regulatory landscape, architectural compatibility, etc.
- Organizational considerations: who should be involved from what functions
- A clearly defined project scope
- Project deliverables, in terms of process and functionality
- Necessary resources, in terms of cost and people
- Analysis of the risks regarding the viability of partners or vendors
- Measurement or likelihood of success
Planning & Requirements

- Ensure key user groups have input
- Requirements meet users needs
- Key controls identified
- Deliverables:
  - Baseline project plan
  - Initial WBS
  - Baseline overall test & review plan
  - Baseline acceptance test plan
  - Baseline training material and schedule

If Buying......

- Obtain vendor’s last SOC-1 / SOC-2 report
- Obtain list of clients using software
- Make contact with their auditors and discuss any issues / concerns / controls
- Review technical requirements for controls
- Ensure IT Security is reviewing the security protocols
- If externally hosted:
  - “pen test” results
  - Right to audit clause
Logical Design

Conduct
- Internal / stakeholder reviews

Define
- Error identification / correction
- Security requirements

Deliverables
- Approved requirements
- Baseline detailed system requirements
- Baseline logical design
- Baseline system test plan

Logical Design

Controls need to be designed into the system
- Security
- Balancing
- Edits
- Quality Assurance
- Output
- Database Administration
Truth?

Projects NEVER have scope changes

Definition - Issue, Change, Problem, Risk

<table>
<thead>
<tr>
<th>Item</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue</td>
<td>Items that are identified as problems or that need more research. They are not straightforward questions, action items, or planned tasks not yet completed. Some items, after analysis, may be reclassified as changes, problems, or risks</td>
</tr>
<tr>
<td>Change</td>
<td>Changes are broadly defined as those activities not originally considered within either the products to be delivered or tasks to be performed as defined by the Project Charter or Project Management Plan</td>
</tr>
<tr>
<td>Problem</td>
<td>Problems are deviations in a product's behavior from that prescribed in the baseline specification</td>
</tr>
<tr>
<td>Risk</td>
<td>Any issue, concern, uncertainty, or potential problem that can adversely affect project technical, cost, or schedule performance</td>
</tr>
</tbody>
</table>
The Triple Constraint

Scope

Quality

Schedule

Cost

Scope Changes

- New government standards/regulations
- Business unit re-organized
- New technology available
- New/different functionality desired
- Vendors can’t support application
- New opportunities revealed
- Smarter about project
Scope Change is...

- A normal part of project management
- Inevitable reality
- Not “good” or “bad”
- Often an opportunity to better serve the end-user
- Responsibility of all stakeholders

Scope “Change” May Mean

- Exceeding budgets
- Late projects
- Inability to meet requirements
- Inability to meeting expectations
- Unhappy:
  - Users
  - Management
  - Project team
**Scope Control**

- Must have a process
- Must have a baseline
- Must be addressed formally
  - In writing (verbal agreements “never happened”)
  - Must be addressed prior to doing the work
- Must be understood up-front

**Managing Change Is All About…**

- Initiating the change
- Assessing change impacts
- Communicating the analysis results
- Negotiating for win-win
- Replanning
- Getting authorization
Change Control - “The Process”

- Identifies who analyzes and authorizes changes for each baseline
- Business owner involvement particularly important
- Authorization normally by business owner or project manager
- Business owner may establish a fund for minor changes
- Should include a definition of “out-of-scope”
- Should define the reports, support tools and expected audits

Change Request Life Cycle

- Change Request
  - Evaluate New Request
  - Identified
    - Evaluate for Investigation
    - Assessed
      - Evaluate for Authorization
      - Authorized
        - Assign Change
        - Assigned For Investigation
          - Complete Investigation
          - Authorize Implementation
            - Authorized For Implementation
              - Implement Change
                - Completed

- Evaluate for Investigation
- Complete Investigation
- Authorize Implementation
- Implement Change
- Completed
Truth?

Projects NEVER have issues

Definition - Issue, Change, Problem, Risk

<table>
<thead>
<tr>
<th>Item</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue</td>
<td>Items that are identified as problems or that need more research. They are not straightforward questions, action items, or planned tasks not yet completed. Some items, after analysis, may be reclassified as changes, problems, or risks</td>
</tr>
<tr>
<td>Change</td>
<td>Changes are broadly defined as those activities not originally considered within either the products to be delivered or tasks to be performed as defined by the Project Charter or Project Management Plan</td>
</tr>
<tr>
<td>Problem</td>
<td>Problems are deviations in a product's behavior from that prescribed in the baseline specification</td>
</tr>
<tr>
<td>Risk</td>
<td>Any issue, concern, uncertainty, or potential problem that can adversely affect project technical, cost, or schedule performance</td>
</tr>
</tbody>
</table>
Causes

Potential Causes of Issues

- Staffing Levels
- Skill Sets
- Inadequate Funding
- Experience
- Stakeholder Involvement

Issue Management - Purpose

To formally identify, explain, assign responsibility for and track issues needing resolution

To provide a control mechanism to ensure that project-related issues are being addressed
Issue Management Plan

- Documents the processes that will be used for issue:
  - Identification
  - Tracking
  - Escalation

- Issue Management Plan should be tailored to meet business requirements

Issue Management - Process

1. Issue submission
   - Prepare issue report
   - Identify issue
   - Identify potential resolution

2. Issue review
   - Review resolved issues
   - Review open and overdue issues
   - Review, prioritize, document new issues in issue log

3. Issue resolution
   - Resolve the issue
   - Report resolution
   - Obtain approval from review meeting committee
4. Issue Tracking
• Maintain Issue Log

5. Issue Escalation
• High Priority
• Significant impact on scope or budget

Issue Log

Use issue log to track and report issues

<table>
<thead>
<tr>
<th>Issue log should include:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue number and name</td>
</tr>
<tr>
<td>Priority</td>
</tr>
<tr>
<td>Person responsible</td>
</tr>
<tr>
<td>Date identified</td>
</tr>
<tr>
<td>Due date</td>
</tr>
<tr>
<td>Date closed</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Resolution</td>
</tr>
</tbody>
</table>
Be Sure to Include….

How issues will be recorded and how status will be monitored including:
- How business owners & project managers will be involved in issue management
- How the issue’s originator will be kept informed about progress towards resolution
- How the status of an issue can be determined

How the resolution of critical issues will be escalated
- Who is involved
- What qualifies as a critical issue
- When escalation is performed

Truth?

Projects NEVER have risks
Definition - Issue, Change, Problem, Risk

<table>
<thead>
<tr>
<th>Item</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue</td>
<td>Items that are identified as problems or that need more research. They are not straightforward questions, action items, or planned tasks not yet completed. Some items, after analysis, may be reclassified as changes, problems, or risks</td>
</tr>
<tr>
<td>Change</td>
<td>Changes are broadly defined as those activities not originally considered within either the products to be delivered or tasks to be performed as defined by the Project Charter or Project Management Plan</td>
</tr>
<tr>
<td>Problem</td>
<td>Problems are deviations in a product’s behavior from that prescribed in the baseline specification</td>
</tr>
<tr>
<td>Risk</td>
<td>Any issue, concern, uncertainty, or potential problem that can adversely affect project technical, cost, or schedule performance</td>
</tr>
</tbody>
</table>

Risk Worksheet

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Failure Mode</th>
<th>Failure Effects</th>
<th>Causes</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training materials will not be received from the outside vendor in time</td>
<td>Materials are delivered late</td>
<td>Training could be delayed or canceled</td>
<td>Giving the material to vendor too late or the vendor is not a known quantity to company</td>
<td>Send the material ASAP and call the vendor periodically</td>
</tr>
<tr>
<td>Personnel assigned to training classes will not be available or actually show up</td>
<td>Not on the system</td>
<td></td>
<td></td>
<td>Reminder notifications to users and managers</td>
</tr>
</tbody>
</table>

Risk Priority Number = Severity x Occurrence x Detection

60 = 5 x 4 x 3
### Mitigation Plan

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Action</th>
<th>Resp</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>May be process step, general activity, functional area, or other rational</td>
<td>What specific actions are required to improve the RPN number</td>
<td>Who will be accountable for</td>
<td>When is completion of the action required or</td>
</tr>
<tr>
<td>grouping</td>
<td></td>
<td>implementing the change</td>
<td>planned</td>
</tr>
<tr>
<td>Training materials will not be received from the outside vendor in time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel assigned to training classes will not be available or actually</td>
<td>Have Business owner or Project Executive send E-mail stressing the</td>
<td>Business Owner with the</td>
<td>By the date training begins and possibly</td>
</tr>
<tr>
<td>show up</td>
<td>need for training</td>
<td>Project Manager</td>
<td>thereafter</td>
</tr>
</tbody>
</table>

### Physical Design

- **Review**
  - Detailed system design, integration test plan and test cases, and system test plan

- **Conduct**
  - Internal / stakeholder reviews
  - Review of sign-off / approval

- **Deliverables**
  - Baseline detailed system requirements
  - Baseline physical design
  - Baseline system test plan
Construction & Unit Test

- Review unit test plans for completeness
- Testing of all key controls, balancing, etc.
- Deliverables:
  - Baseline system design / code
  - Baseline unit test plan and test cases

System & Acceptance Testing

- Review test plans for completeness
- Ensure mapping of requirements to test cases / results
- Training material testing
- If conversion, control totals and processes
- Cyclical processing: daily, weekly, monthly, quarterly, year-end, roll-over (year to year)
- Manual processes developed and tested
The Trace Matrix

Testing Nightmare

Original Testing Schedule

Revised Testing Schedule

ACTUAL Testing
System & Acceptance Testing

- Parallel testing plans / results
- Security modules tested
- Test errors / retesting
- Training plans executed
- Backout protocols

Audit Testing Guidance
- If time is decreased by 10%, Project Executive must approve

Deliverables:
- Sign-off for System Test
- Sign-off for Acceptance Test
- Updated test case artifacts
Production Preparation

• Operational test plan and test cases
• Completeness of system documentation – sign off by QA
• All users (IT and non-IT) trained
• All retesting completed
• High Risk issues resolved
• Deliverables:
  • Baseline operational test plan
  • Baseline operational test cases

Installation / Post Installation

• Review programmed procedures for scheduling and running application in production
• Approval by QA to move into production
• Help Desk fully trained
• Deliverables:
  • Completed Project closeout document
  • Deployed work product
  • Completed operational test case
  • Documented lessons learned
“Change” Management

Change management is a systematic approach to dealing with change, both from the perspective of an organization and on the individual level.

- The most underestimated aspect
  - Change in business processes or workflow
  - Implementation of new system
  - Communication must occur throughout
  - Clear and concise objectives
  - Elevator talking points
  - Training is timely and adequate
  - Post-launch support is defined for both functional and technical aspects

Agenda

- Audit Basics
- The Need / The Risks
- Types of Engagements
- Advisory Services
- Reporting
Engagement Announcement

The Claims Customer Service Process (CCSP) program has been selected for review by ITAAS based upon the program scope and ITAAS risk assessment.

**Planning:**
In preparation for this engagement, we have reviewed available CCSP program information, including business cases for CCSP [sic] projects, presentations made to various groups within HCSC. In addition, meetings were held with project leadership to understand their view of risk within the program and its projects.

**Objectives:**
The objective of this engagement is to identify areas of potential risk or audit concern within the CCSP program, and to assess the controls in place surrounding the risks and concerns identified. The Advisory Engagement will focus on risks/concerns at both the program level, and within the individual projects under the CCSP program.

This engagement will also employ an integrated advisory approach: a collaboration between the IT and Operational advisory teams within Audit.

**Audit Scope**
Given the expansive and complexity of the CCSP Initiative, scope is presented at two levels including, but not limited to, the following:

**Program Level:** Elements to be reviewed and assessed from the overall program perspective. Guidance statements and improvement opportunities would pertain to the overall program, as well as to all projects under the CCSP program umbrella.

**Program Level Scope**
- Compliance to HCSC Corporate policies and standards
- Vendor management
- Status reporting
- Monitor changes to controls tested by End-of-Year and SAS70 external auditors
### Engagement Announcement

**Project Level:** Elements of scope may be applied to one or more projects under the OCSP program, and any Guidance statements or Improvement Opportunities would specify the project(s) they address.

**Project Level Scope**
- System and operational documentation
- Testing strategy and execution controls
- Operational process review
- System Interface controls

In addition, ITAMS may review additional areas of risk or concern identified during the engagement. ITAMS will communicate and discuss with CCSF leadership any newly identified risk concerns prior to changing the scope or objective of the engagement.

**Proposed Engagement Milestone Dates and Assigned Auditors**

<table>
<thead>
<tr>
<th>Engagement Milestone</th>
<th>Beginning Date</th>
<th>Ending Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engage Project re: Scope Areas of Review</td>
<td>4/6/08</td>
<td>12/31/08</td>
</tr>
<tr>
<td>Conduct Interim Status Meetings</td>
<td>4/30/08</td>
<td>12/31/08</td>
</tr>
<tr>
<td>Issue Engagement Closing Summary**</td>
<td>1/30/09</td>
<td>1/30/09</td>
</tr>
</tbody>
</table>

### Improvement Opportunity Document - IOD

**Advisory Engagement Title**
*Improvement Opportunity Document*

- **Improvement Opportunity Title:** (Use simple, clear opportunity name)
- **IOD Number:** (List the number for the IOD issued)
- **Date Released:** (MM/DD/YYYY)

**Observations:**
- Describe the scenario that elicited the opportunity. Cite any documentation or evidence for issuing the IOD, include specific details, observations or project documentation sources available.

**Recommendations:**
- Document possible solution(s) to address the scenario described in ‘Observations’.

**Potential Benefit:**
- Describe the benefit to the project by addressing the identified opportunity; include risks that may be mitigated by the project response.

**Response/Action Plan:**
- Response provided by project sponsor and/or business lead. This should include a due date.

**Primary Responsible Area:**
- Response provided by project sponsor and/or business lead. This should be the business area that is accountable for completing the improvement plan. Sometimes this varies from the person who provides the response/action plan.

**Status:**
- Open, Pending, Closed
- Due Date: (MM/DD/YYYY)
Project Guidance

• Statement of guidance regarding potential risk or control concern
• Provides audit “point of view” on project activities and issues
• Provided before risk or control has a negative impact
• Includes analysis and recommendation for preventative action
• Requires a response
• Can be requested by the project directly
### Project Guidance

**Advisory Engagement - Project Guidance**

<table>
<thead>
<tr>
<th>Guidance Title:</th>
<th>Account Setup Compliance Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor(s):</td>
<td>Lead Auditor</td>
</tr>
<tr>
<td>Engagement:</td>
<td>ASO/BARS Rewrite</td>
</tr>
<tr>
<td>Released:</td>
<td>04/05/2005</td>
</tr>
<tr>
<td>Sponsor:</td>
<td>Eric Sponsors</td>
</tr>
<tr>
<td>Copied to:</td>
<td>Project Leads</td>
</tr>
</tbody>
</table>

**Engagement Details:**

The objective of the Account Billing Set-up Advisory Engagement is to identify areas of potential risk or audit concern within the ASO/BARS Rewrite project lifecycle.

**Risk/Control Addressed:**

As new functionality is deployed, the operational and system controls required for MAR (Module Audit Rule) compliance should be implemented. Core process controls required to achieve Audit compliance are managed and transitioned as roles switch from one area of ownership to another to provide a sustainable control solution.

**Analysis Details:**

MAR and SAS-70 assessments require ASO account setup processes be adequately controlled. As account setup process ownership is transitioning from the Finance area to the Marketing area, roles within the enterprise are expected to change impacting control activity documentation. Overall compliance, and accountability for control effectiveness, is now a responsibility of the Marketing area.

**Guidance:**

It is recommended that Marketing and the project team review the controls and objectives to satisfy MAR and SAS 70 below. Marketing should work with the project team to develop operational processes that adhere to these controls. These controls should result in proper documentation which includes future evidence required to support and pass an audit. To date, no audit findings exist related to the ownership or maintenance of these controls in Compliance 360. However, it is essential that updates to ownership and control reviews be completed for the MAR matrices.

**MAR Audit General Controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Control 100</td>
<td>Only groups approved by Underwriting are set up for processing in BARS.</td>
</tr>
<tr>
<td>Control 110</td>
<td>Inputted rates are accurately entered into BARS in a timely manner.</td>
</tr>
</tbody>
</table>

**Ernst and Young - SAS 70 Controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Objective 8</td>
<td>Controls provide a reasonable assurance that outputs are accurate.</td>
</tr>
</tbody>
</table>

---

### Status Report

**AUDIT SERVICES**

**Advisory Engagement Status Report**

<table>
<thead>
<tr>
<th>Engagement Name</th>
<th>Project Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditors</td>
<td>Auditor Name, Business Area, Names of Team Members</td>
</tr>
<tr>
<td>Tenure</td>
<td>IS Audit Team, Audit Report Center</td>
</tr>
</tbody>
</table>
| Goal            | IS Audit Team, Report copied for | 35:35%

<table>
<thead>
<tr>
<th>Review Period</th>
<th>Quarter, YYYY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Summarize the objective and scope of the engagement including any refinement, as appropriate.</td>
</tr>
<tr>
<td>Work Performed</td>
<td>To date, this has involved 100 hours towards the audit initiative. During the course of this review period, the following work was completed:</td>
</tr>
<tr>
<td>- Projected 20 activities ongoing advisory effort.</td>
<td></td>
</tr>
</tbody>
</table>

**Improvement Opportunities, Project Guidance and Observations**

**Improvement Opportunities**

- Identify key steps for the implementation of the project.
- Identify key areas for improvement during the previous status period.

**Project Guidance**

- During the course of this review period, the following guidance documents were issued to the project team:
- Key control should be included in master project plan. At least one observation should be included.

**Observations**

- During the course of this review period, the following observations were made:
- Key control should be included in master project plan. At least one observation should be included.

**Planned Activities**

During the course of the next review period (Quarter, YYYY), the following work will be completed:

- Activities during previous quarter
- IODS and Guidance issued
- Planned activities

---

**Status Reports**

- **Engagement update targeted to key project stakeholders and project leadership (up to ELG)**
- **Enhanced awareness during long projects**
- **Provides senior management information on engagement progress or issues observed by IT Audit**
- **Includes brief summary of:**
  - Activities during previous quarter
  - IODS and Guidance issued
  - Planned activities
## Advisory Engagement Status Report

<table>
<thead>
<tr>
<th><strong>Engagement Name:</strong></th>
<th>CCSP 2010 Advisory Engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auditors:</strong></td>
<td>Various Business ITG &amp; SSD</td>
</tr>
<tr>
<td><strong>To:</strong></td>
<td>Project Leads</td>
</tr>
<tr>
<td><strong>Cc:</strong></td>
<td>Audit Management</td>
</tr>
<tr>
<td><strong>Review Period:</strong></td>
<td>2nd Quarter 2010</td>
</tr>
<tr>
<td><strong>Release Date:</strong></td>
<td>7/19/2010</td>
</tr>
</tbody>
</table>

### Objectives and Scope of Engagement

The 2010 CCSP Advisory Engagement will initially review the following areas:

#### IT Scope:
- **Control Inventory** - Ongoing assessment of identified production IT controls impacted by CCSP that support SAS70, end of year financial or MAR compliance engagements.
- **System Retirement** - Identification of systems and related processes being retired as a result of the CCSP program to identify impacts to current IT controls.
- **Disaster Recovery** - Review of current disaster recovery plans to ensure CCSP delivered systems are supported by disaster recovery plans and tested during annual disaster recovery exercises.
- **E&Y Updates** - Ongoing delivery of CCSP project information to external engagement partners and HCSC Corporate Governance supporting SAS70, end of year financial and MAR compliance engagements.

#### Operational Focus:
- **Control Inventory** - Assessment of the operational controls impacted by CCSP that will affect processes that are documented with Corporate Governance.
- **System Retirement** - System, processes or any applicable controls that are retired are adequately covered in other systems or other controls.
- **E&Y Updates** - Ongoing delivery of CCSP project information to external partners and HCSC Corporate Governance supporting SAS70, end of year financial and MAR compliance engagements, as we are made aware.

As 2010 progresses, additional elements of scope may be identified and communicated to CCSP Leadership to provide a more timely and relevant engagement throughout the year.

---

## Status Report

### Review of Work Performed

To date, Audit Services has invested 340 hours towards this 800 hour engagement. During the course of this review period the following work was completed:

**DB2**

ITAAS met with the DB2 project team on 4/22/10 to discuss the implementation of a second claims database in DB2. The discussion focused on the DB engine program structure, how it will write to both legacy and DB2 databases, and how it be assured both databases are updated correctly. DB2 project team indicated that a "comparison view" was available between both databases; a program that showed side-by-side, how each datum is written to both platforms. However, this is a view available to programmers and is not user friendly. Further, the view is not automated and is not designed as a reporting vehicle or assurance mechanism.

**Operational Focus**

Audit Services presented the Program Leadership Team with an inventory of MAR processes that may change due to current and future CCSP projects. Audit Services will work with the Program Leadership Team and business areas to identify any anticipated changes to these MAR processes and identify others that may be affected. The Program Leadership team is also exploring the idea of having a point person in SSD that will be the intermediary between SSD Tech and the business areas in order to exchange information on the CCSP project. In addition a review of future and current audits that cover these processes will be completed and updates communicated to the audit team, as necessary.
Status Report

Improvement Opportunities and Project Guidance

Improvement Opportunities
No Improvement Opportunity (IOD) documents were issued during the course of this review period.

Project Guidance
No Project Guidance was issued during the course of this review period.

Planned Activities
During the course of the next review period (3rd Quarter, 2010), the following work will be completed:

- Continued discussion of RTIS "interface" controls, specifically the balancing of claims in a state-based adjudication environment
- Obtaining testing understanding of the DB2 project including understanding of comparison views available and testing plans
- Engaging the CCSP program to understand security controls assessed by external partners to support control inventory efforts
- Continue to identify and assess control designs within CCSP-delivered systems that support SAS70 control objectives.

Closing Summary

AUDIT SERVICES

Proxy Re-Write

Engagement Closing Summary - FINAL

January 1, 2009

- Engagement Closing Summary
- Developed upon completion of the engagement
- Released to project leadership, up to first level of ELG management
- Summary includes the following components:
  - Background
  - Objective
  - Scope
  - Summary of Work Performed
  - Conclusion
  - Formal End of Engagement
Closing Summary

BACKGROUND:
In 2006, IT Audit & Advisory Services (ITAS) engaged Information Technology Protection Services (ITPS) regarding the enterprise Distributed Environment Cleanup initiative. The focus of our engagement was to assist ITPS during the identification and remediation of user access in targeted distributed environments. Novell NetWare, a core technology platform for HCSC, is used to manage network user authentication and password controls, data storage/security, and printer services and is managed and administered by ITPS.

The 2006 cleanup effort of Novell was significant. Over 3,000 user IDs were either deleted or disabled as a result of ITPS remediation efforts. Equally important is to ensure the Novell environment continues to reflect the remediated state, making it vital that ongoing sustainment processes are developed and monitored for effectiveness. The viability of Novell configuration standards with internal and external auditors, and the strategic importance of the technology to HCSC, warranted continuous monitoring by ITAS.

OBJECTIVE:
The objective of this engagement is to assess the effectiveness of ITPS Novell configuration management processes by measuring compliance with existing Corporate and ITPS standards on a quarterly basis throughout 2007.

SCOPE:
The scope of this engagement included a quarterly evaluation of all uniquely assigned Novell user IDs to assess the following attributes’ compliance to identified standards in the production environment:
- User ID Expiration Date
- Maximum User ID Concurrent Login Setting
- Password Required Setting

ENGAGEMENT SUMMARY:
Based upon the analysis performed, HCSC experienced a steady growth of Novell User IDs under management each quarter. The overall number of disabled IDs increased throughout 2007, with the most notable jump in disabled IDs occurring during the 4th quarter, indicating efforts on the part of ITPS to maintain compliance while managing overall user growth.

Closing Summary

Five Improvement Opportunity Documents (IOD) were released with the 3rd quarter Status Report addressing a number of Novell attributes in which exceptions persisted throughout the year. ITPS provided a remediation plan to address the exceptions. However, the plan was not completed by the date provided by ITPS. In addition, it was observed that new non-compliant Novell accounts were introduced during the 4th quarter of 2007, indicating controls surrounding Novell account administration require improvement and/or enhanced monitoring capabilities.

ENGAGEMENT CONCLUSION:
The majority of Novell User ID attributes analyzed were found to be above the target compliance threshold of 95%. However, the Concurrent Login attribute was not in compliance during 2007, and was not successfully remediated in response to the related IOD. Coupled with the trend of 5 out of 6 attributes exhibiting a decrease in compliance during 2007, ITAS has determined that continued monitoring is merited.

ITAS will continue to monitor Novell User ID attributes in 2008 until analysis indicates two consecutive quarters in which all monitored attributes are determined to be above the 95% compliance threshold and that compliance levels remain consistent or improved.

Lastly, the IOD’s issued during the course of this engagement are attached at the end of this report for reference purposes.