COBIT & ITIL usage for SOX - current and future

Robert E Stroud
International Vice President ISACA
Evangelist ITSM & IT Governance CA, Inc.

Japan, November 8, 2007
Trademark Notice

ITIL® is a registered trademark and a registered community trademark of the UK Office of Government and Commerce (OGC) and is registered in the U.S. Patent and Trademark Office.
COBIT® is a registered trademark of ISACA/ITGI - Information Systems Audit and Control Association / IT Governance Institute®

DISCLAIMER
ITGI, CA nor the speaker warrant or guarantee the concepts or the accuracy of information provided herein.

© All rights reserved

No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission of the author and ITGI, Japan.
Robert Stroud

• 26 years Industry Experience
• 15+ years Banking Industry
• IT Governance
  – International Vice President ISACA¥ITGI
  – Chair COBIT Steering Committee
  – Member ITGC
  – Contributor to COBIT V4 and V4.1
  – Contributor to Basel II Guidance
• ITSM
  – itSMF USA Board of Directors
  – Chair itSMF USA Certification Committee
  – Member ITIL V3 Advisory Group
  – Mentor ITIL V3 Service Transition
  – Reviewer ITIL V3
  – Contributor ITIL Business Perspectives Volume II
  – Author ITIL¥COBIT¥ISO17799 Management Overview
Agenda

• Frameworks
  – COBIT
  – ITIL
  – ISO/IEC 20000
• USING COBIT with ITIL
• Summary
Agenda

- SOX and JSOX
- Frameworks
  - COBIT
  - ITIL
  - ISO/IEC 20000
- USING COBIT with ITIL
- Practical experience
- Summary
What is COBIT®?

• **Control Objectives for Information and related Technology**
• A framework for IT governance
• Bridges the gaps between business risks, control needs and technical issues
• Documents good (best) practices
• Increasing Global 2000 adoption
• Compliance has lead to increasing use.....
COBIT Evolution

Current Version 4.1

Evolution

- Governance
- Management
- Control
- Audit

COBIT 1 (1996)
COBIT 2 (1998)
COBIT 3 (2000)
COBIT 4 (2005)
Top-down approach

Enterprise Strategy

Business Strategy for IT

IT Goals

Enterprise Architecture for IT

IT Scorecard

define

measure
How Do Governance and the Business Drive IT?

- Business Goals
  - Governance Drivers
  - Business Outcomes

  - Applications
  - Information
  - Infrastructure
  - People

- IT Goals
- IT Processes
Governance Drivers

Information Criteria
• Effectiveness
• Efficiency
• Confidentiality
• Integrity
• Availability
• Compliance
• Reliability

IT RESOURCES
• Applications
• Information
• Infrastructure
• People

Business Goals

MONITOR AND EVALUATE

Plan and Organise

Acquire and Implement

Deliver and Support

PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define the IT processes, organisation and relationships
PO5 Manage the IT investment
PO6 Communicate management aims & direction
PO7 Manage IT human resources
PO8 Manage quality
PO9 Assess and manage risks
PO10 Manage projects

AI1 Identify automated solutions
AI2 Acquire and maintain application software
AI3 Acquire & maintain technology infrastructure
AI4 Enable operation and use
AI5 Procure IT resources
AI6 Manage changes
AI7 Install and accredit solutions and changes

ME1 Monitor & evaluate IT performance
ME2 Monitor & evaluate internal control
ME3 Ensure regulatory compliance
ME4 Provide IT governance

DS1 Define service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and attribute costs
DS7 Educate and train users
DS8 Manage service desk and incidents
DS9 Manage the configuration
DS10 Manage problems
DS11 Manage data
DS12 Manage the physical environment
DS13 Manage operations
A16 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This ensures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy; whilst reducing solution and service delivery defects and rework

by focusing on

controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications and halting implementation of unauthorised changes

is achieved by

• Defining and communicating change procedures, including emergency changes
• Assessing, prioritising and authorising changes
• Tracking status and reporting on changes

and is measured by

• Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
• Application or infrastructure rework caused by inadequate change specifications
• Percent of changes that follow formal change control processes
Detailed Control Objectives

Detailed Control Objectives

A16 Manage Changes

A16.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

A16.2 Impact Assessment, Prioritisation and Authorisation
Ensure that all requests for change are assessed in a structured way for impacts on the operational system and its functionality. This assessment should include categorisation and prioritisation of changes. Prior to migration to production, changes are authorised by the appropriate stakeholder.

A16.3 Emergency Changes
Establish a process for defining, raising, assessing and authorising emergency changes that do not follow the established change process. Documentation and testing should be performed, possibly after implementation of the emergency change.

A16.4 Change Status Tracking and Reporting
Establish a tracking and reporting system for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.

A16.5 Change Closure and Documentation
Whenever system changes are implemented, update the associated system and user documentation and procedures accordingly. Establish a review process to ensure complete implementation of changes.
AI6 – Manage Changes

• All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment..

• Control over the IT Process of
  – Manage Changes
  – that satisfies the business requirement for IT of responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework
  – by focusing on
  – controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions; minimising errors due to incomplete request specifications; and halting implementation of unauthorised changes
    – is achieved by
    – Defining and communicating change procedures, including emergency changes
    – Assessing, prioritising and authorising change
    – Tracking status and reporting on changes
  – and is measured by
    • Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
    • Amount of application or infrastructure rework caused by inadequate change specifications
    • Percent of changes that follow formal change control processes
### Management Guidelines

#### A16 Manage Changes

<table>
<thead>
<tr>
<th>From</th>
<th>Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>IT project portfolio</td>
</tr>
<tr>
<td>P08</td>
<td>Quality improvement actions</td>
</tr>
<tr>
<td>P09</td>
<td>IT-related risk remedial action plans</td>
</tr>
<tr>
<td>P010</td>
<td>Project management guidelines and detailed project plan</td>
</tr>
<tr>
<td>DS3</td>
<td>Required changes</td>
</tr>
<tr>
<td>DS5</td>
<td>Required security changes</td>
</tr>
<tr>
<td>DS8</td>
<td>Service requests/requests for change</td>
</tr>
<tr>
<td>DS9-10</td>
<td>Requests for change (where and how to apply the fix)</td>
</tr>
<tr>
<td>DS10</td>
<td>Problem records</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Change process description</td>
</tr>
<tr>
<td></td>
<td>Change status reports</td>
</tr>
<tr>
<td></td>
<td>Change authorisation</td>
</tr>
</tbody>
</table>

#### RACI Chart

<table>
<thead>
<tr>
<th>Activities</th>
<th>CEO</th>
<th>CFO</th>
<th>Business Executive</th>
<th>Business Process Owner</th>
<th>Head Operations</th>
<th>Chief Architect</th>
<th>Head Development</th>
<th>Head IT Administration</th>
<th>PINO</th>
<th>Compliance, Audit, Risk and Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop and implement a process to consistently record,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>assess and prioritise change requests.</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Assess impact and prioritise changes based on business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>needs.</td>
<td>I</td>
<td>R</td>
<td>A/R</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Assure that any emergency and critical change follows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the approved process.</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
<td>I</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorise changes.</td>
<td>I</td>
<td>C</td>
<td>A/R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage and disseminate relevant information regarding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>changes.</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.
Goals and Metrics

Activity Goals
- Defining and communicating change procedures including emergency changes and patches
- Assessing, prioritising and authorising changes
- Scheduling changes
- Tracking status and reporting on changes

Process Goals
- Make authorised changes to the IT infrastructure and applications.
- Assess the impact of changes to the IT infrastructure, applications and technical solutions.
- Track and report change status to key stakeholders.
- Minimise errors due to incomplete request specifications.

IT Goals
- Respond to business requirements in alignment with the business strategy.
- Reduce solution and service delivery defects and rework.
- Ensure minimum business impact in the event of an IT service disruption or change.
- Define how business functional and control requirements are translated in effective and efficient automated solutions.
- Maintain the integrity of information and processing infrastructure.

Key Performance Indicators
- % of changes recorded and tracked with automated tools
- % of changes that follow formal change control processes
- Ratio of accepted to refused change requests
- # of different versions of each business application or infrastructure being maintained
- # and type of emergency changes to the infrastructure components
- # and type of patches to the infrastructure components

Process Key Goal Indicators
- Application rework caused by inadequate change specifications
- Reduced time and effort required to make changes
- % of total changes that are emergency fixes
- % of unsuccessful changes to the infrastructure due to inadequate change specifications
- # of changes not formally tracked or not reported or not authorised
- Backlog in the number of change requests

IT Key Goal Indicators
- # of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
COBIT Maturity Model

Maturity Model

AI6 Acquire and Implement
Manage Changes

AI6 Manage Changes

Management of the process of Manage changes that satisfies the business requirement for IT of responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework is:

0 Non-existent when
There is no defined change management process and changes can be made with virtually no control. There is no awareness that change can be disruptive for IT and business operations, and no awareness of the benefits of good change management.

1 Initial/Ad Hoc when
It is recognised that changes should be managed and controlled. Practices vary and it is likely that unauthorised changes take place. There is poor or non-existent documentation of change, and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

2 Repeatable but Intuitive when
There is an informal change management process in place and most changes follow this approach; however, it is unstructured, rudimentary and prone to error. Configuration documentation accuracy is inconsistent and only limited planning and impact assessment takes place prior to a change.

3 Defined Process when
There is a defined formal change management process in place, including categorisation, prioritisation, emergency procedures, change authorisation and release management, and compliance is emerging. Workarounds take place and processes are often bypassed. Errors may still occur and unauthorised changes occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalised, to support planned rollouts of new applications and technologies.

4 Managed and Measurable when
The change management process is well developed and consistently followed for all changes, and management is confident that there are minimal exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimise the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation are becoming more integrated with changes in the business processes, to ensure that training, organisational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process redesign. There is a consistent process for monitoring the quality and performance of the change management process.

5 Optimised when
The change management process is regularly reviewed and updated to stay in line with good practices. The review process reflects the outcome of monitoring. Configuration information is computer-based and provides version control. Tracking of changes is sophisticated and includes tools to detect unauthorised and unlicensed software. IT change management is integrated with business change management to ensure that IT is an enabler in increasing productivity and creating new business opportunities for the organisation.
3 – Defined when
There is a defined formal change management process in place, including categorisation, prioritisation, emergency procedures, change authorisation and release management, and compliance is emerging. Workarounds take place, and processes are often bypassed. Errors may occur and unauthorised changes occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalised, to support planned rollouts of new applications and technologies.
## Maturity Levels in COBIT

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Management processes are not applied at all.</td>
</tr>
<tr>
<td>1</td>
<td>Processes are <em>ad hoc</em> and disorganised.</td>
</tr>
<tr>
<td>2</td>
<td>Processes follow a regular pattern.</td>
</tr>
<tr>
<td>3</td>
<td>Processes are documented and communicated.</td>
</tr>
<tr>
<td>4</td>
<td>Processes are monitored and measured.</td>
</tr>
<tr>
<td>5</td>
<td>Best practices are followed and automated.</td>
</tr>
</tbody>
</table>
Process Controls

❖ 6 control principles that apply to every process
❖ Enabled streamlining of 4.0
❖ Verified and enhanced for 4.1

PC1 Process Goals and Objectives
PC2 Process Ownership
PC3 Process Repeatability
PC4 Roles and Responsibilities
PC5 Policy, Plans and Procedures
PC6 Process Performance Improvement
Application Controls

- Moved from 18 to 6
- Removed manual controls
- Moved security controls
- Consolidated and enhanced

AC1 Source Data Preparation and Authorisation
AC2 Source Data Collection and Entry
AC3 Accuracy, Completeness and Authenticity Checks
AC4 Processing Integrity and Validity
AC5 Output Review, Reconciliation and Error Handling
AC6 Transaction Authentication and Integrity
Documentation usage

* Board Briefing on IT Governance, 2nd Edition
IT Control Practices and Assurance Steps

Control design
- Necessary and sufficient steps
- Roles & responsibilities
- Characteristics
- Generic and specific
- Active and passive
- Inputs, outputs, activities

Business and IT Goals

Scoping

Test approach
- at the process level
- at the control objective level
- at the control practice level
- distinct for application and general controls

IT Assurance Framework
- Four Test objectives
- Five Test techniques
- Three Assurance Objectives
  1. Control design
  2. Objective outcome
  3. Weakness impact

Control Objective
Value
Risk
Control Practices
Assurance Approach
Agenda

• SOX and JSOX
• Frameworks
  – COBIT
  – ITIL
  – ISO/IEC 20000
• USING COBIT with ITIL
• Practical experience
• Summary
What Is ITIL®?

• IT Infrastructure Library
• An integrated best practice for the Service Lifecycle Management of IT enabled services
• The de-facto standard in IT Service Management
• A framework developed by the UK’s Office of Government Commerce (OGC) captured in a series of books
ITIL Evolution

• Late 1980s
  – UK government project started
  – CCTA (OGC) involved in development plus practitioner and consulting organizations
  – First books published

• Early 1990s
  – The library completed

• Late 1990s
  – Generally accepted as the de-facto standard for IT service management worldwide
  – Introduced ITIL to North America

• 2000-2005
  – Submission to ISO/IEC20000 – fast tracked and accepted
  – Vendor community supports ITIL and are developing products and practices in support of
    the framework
  – ITIL Version 3 commenced

• 2006
  – ITIL – a defacto global standard

• 2007
  – ITIL Version 3 released
Planning to Implement Service Management

Service Management

- Service Support
- Service Delivery
- Security Management

The Business Perspective

Applications Management

ICT Infrastructure Management

The Business Perspective 2

Software Asset Management

The Magnificent Nine, Ten etc
Version 2 – 10 books, 2 used

• **Service Delivery**
  – Five tactical processes.
  – Describe the services a customer needs and what is needed to provide those services.
  – Transforms IT activities into strategic business value

• **Service Support**
  – Five operational processes and one function (Service Desk)
  – Describe how a customer gains access to support services
  – A foundation upon which to build business value
Change Management Activities

Problem Management Process

Error Control

CMDB

Configuration Management Process

Request For Change

Acceptance And Classification

Assessment And Planning

Authorization Of Changes

Control And Coordination

Evaluation
Release Management

- New Technology
- New Services
- Application Enhancements
- Projects
- Fixes or Time Sensitive issues

Pre Production
- Major Release
- Medium Release
- Minor Release
- Emergency Release

Release Readiness?

RFC

Right Requirements

Change Management
- Testing
- Documentation
- Training
- Acceptance
- Standards
- Support

Promote to Production

Configuration Management
ITIL: 21 Years of Service Improvement

- ITIL Version 3
  - Business-IT service integration and value generation
  - Service Management for business and technology

- ITIL Version 2
  - Business-IT alignment
  - Quality and efficiency of IT processes

- ITIL Version 1
  - Stability and control of IT infrastructure
  - IT Infrastructure Management process
ITIL Changed From V2 To V3

- **V2 Focus: IT to Business Alignment**
  - **Service Support:** support day-to-day activities maintain IT services
  - **Service Delivery:** plan and deliver quality IT services

- **V3 Focus: IT to Business Integration through the Service Lifecycle approach**
Lifecycle Processes

SERVICE STRATEGY
- Service Strategy
- Service Portfolio Management
- Financial Management
- Demand Management

SERVICE DESIGN
- Service Catalog Management
- Service Level Management
- Supplier Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management

SERVICE OPERATION
- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management

CONTINUAL SERVICE IMPROVEMENT
- Seven Step Improvement

SERVICE TRANSITION
- Transition Planning and Support
- Change Management
- Service Asset & Configuration Management
- Release & Deployment Management
- Service Validation
- Evaluation
- Knowledge Management
Agenda

• Frameworks
  – COBIT
  – ITIL
  – ISO/IEC 20000

• USING COBIT with ITIL

• Practical experience

• Summary
What is ISO/IEC 20000?

• Based on the UK standard, BS 15000
• Published as ISO/IEC 20000 in December 2005
  – Part 1 is the ‘must do’ requirements
  – Part 2 is code of practice (advice on Part 1)
• Often referred to as ‘The ITIL standard’
• Management involvement and accountability
• Competence, awareness and training
• Continual improvement
• Introducing services
• ‘Doing not documenting’
Processes covered

Capacity management
Service continuity & availability management
Release management
Change management
Configuration management
Incident management
Problem management
Service level management
Service reporting
Information security management
Budgeting & accounting for IT services
Business relationship management
Supplier management
What is service management?

Manage Services

Management Responsibility

PLAN
Plan service management

DO
Implement Service Management

CHECK
Monitor, Measure and Review

ACT
Continual Improvement

Business requirements

Customer requirements

Request for new or changed services

Other process, business, supplier, customer

Other Teams, eg Security

Business Results

Customer Satisfaction

New or changed service

Other process, business, supplier, customer

Team & People Satisfaction
‘shall’ requirements

• Leadership
• Management commitment
  — Accountability
  — Top-down approach
  — Policy driven
• Integrated processes
• Intelligent use of metrics
Positioning with ITIL

- Real proof of best practices
- Reassurance for the customer
- Common inter-enterprise operational processes
- Ability to manage across a diverse environment
- Improved automation of service management
- Inter-changeability of service providers
- For staff and managers:
  - Common goal
  - Common framework for staff training
  - Inter-changeability of staff
- Reduced risk
ISO/IEC 20000 moving forward

• Links to study group on governance standards
• Part 3 - additional advice
  – Scoping, scope statements, applicability
  – For the service provider
• Parts 1 and 2
  – Integrated management system (with ISO 9001)
  – Alignment between ISO/IEC 20000 and ITIL v 3
  – “Adoption of ITIL can position a service provider to achieve ISO/IEC 20000”
• Harmonisation of standards
Agenda

- Frameworks
  - COBIT
  - ITIL
  - ISO/IEC 20000

- **USING COBIT with ITIL**

- Practical experience

- Summary
IT Models, Standard, best practices

SCOPE OF COVERAGE

WHAT

COBIT

ISO 9000

ITIL

ISO 27000

HOW

COSO
How that fits?

Drivers

Enterprise Governance

Balanced Scorecard

COSO

IT Governance

COBIT

Best Practice Standards

ISO 9000

ISO 27000

ISO 20000

Processes and Procedures

QA Procedures

Security Principles

ITIL
Potential COBIT & ITIL

- Strategic Alignment
- Value Delivery
- Risk Management
- Resource Management
- Performance Measurement

IT Governance Domains

COBIT

ITIL
COBIT & ITIL Mapping

PO: Assess Risk
DS: Define & Manage Service Levels
DS: Manage 3rd Party Services
DS: Manage Performance & Capacity
DS: Ensure Continuous Service
DS: Identify & Allocate Costs
DS: Ensure System Security

AI: Acquire & Maintain Application Software

AI: Manage Change
AI: Install & Accredit Systems

DS: Assist & Advise IT Customers
DS: Manage Problems & Incidents
DS: Manage Configuration

DS: Manage Operations
DS: Manage Facilities
DS: Manage Data

AI: Acquire & Maintain Technology Infrastructure

AI: Acquire & Maintain Application Software
ITIL Books to COBIT Control Objectives

- Service Delivery
  - DS1
  - DS3
  - DS4
  - DS6
  - PO5

- Service Support
  - DS8
  - DS9
  - DS10
  - AI5
  - AI6

- ICT Infrastructure Mgmt
  - AI1
  - AI3
  - PO1
  - PO2
  - PO3
  - PO4
  - PO7

- Application Mgmt
  - AI1
  - AI2
  - AI4
  - PO10
  - PO11

- Security Mgmt
  - M2
  - M3
  - M4
  - PO4
  - PO7
  - PO8

- Planning to Implement Service Mgmt
  - PO4
  - PO6
  - PO7
  - PO11

- Business Perspective
  - PO9
Mapping to ITIL Service Support and Service Delivery

- **Service Management**
- **Service Delivery**
  - Service Level Mgmt
  - Financial Mgmt
  - Availability Mgmt
  - Capacity Mgmt
  - IT Continuity Mgmt
- **Service Support**
  - Configuration Mgmt
  - Incident Mgmt
  - Problem Mgmt
  - Change Mgmt
  - Release Mgmt

DS1, PO5; DS6, DS4, DS3, DS9, DS8, DS10, AI6
COBIT and ITIL compliment each other

COBIT and ITIL together

ITIL
• Best Practice
• Process
• Relationships

COBIT
• Controls Audit
• Requirements
• Maturity Scale

PROCESS/PROCEDURE & RESULTS
Agenda

• Frameworks
  – COBIT
  – ITIL
  – ISO/IEC 20000

• USING COBIT with ITIL

• Practical experience

• Summary
IT Control Objectives for SOX

IT CONTROL OBJECTIVES FOR SARBANES-OXLEY

THE ROLE OF IT IN THE DESIGN AND IMPLEMENTATION OF INTERNAL CONTROL OVER FINANCIAL REPORTING

2ND EDITION

SEPTEMBER 2006
1. Plan & Scope
   - Financial reporting process
   - Supporting systems

2. Perform Risk Assessment
   - Probability & Impact to business
   - Size / complexity

3. Identify Significant Controls
   - Application controls - over initiating, recording, processing & reporting
   - IT General Controls

4. Document Controls
   - Policy manuals
   - Procedures
   - Narratives
   - Flowcharts
   - Configurations
   - Assessment questionnaires

5. Evaluate Control Design
   - Mitigates control risk to an acceptable level
   - Understood by users

6. Evaluate Operational Effectiveness
   - Internal audit
   - Technical testing
   - Self assessment
   - Inquiry +
   - All locations and controls (annual)

7. Determine Material Weaknesses
   - Significant weakness
   - Material weakness
   - Remediation

8. Document Results
   - Coordination with Auditors
   - Internal sign-off (302, 404)
   - Independent sign-off (404)

9. Build Sustainability
   - Internal evaluation
   - External evaluation

Implementation Road Map

- Business Value
- Sarbanes-Oxley Compliance
Mapping PCAOB and COBIT

<table>
<thead>
<tr>
<th>IT Control Objectives for Sarbanes-Oxley</th>
<th>COBIT</th>
<th>PCAOB IT General Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Acquire and maintain application software.</td>
<td>AI2</td>
<td>• • • •</td>
</tr>
<tr>
<td>2. Acquire and maintain technology infrastructure.</td>
<td>AI3</td>
<td>• • •</td>
</tr>
<tr>
<td>3. Enable operations.</td>
<td>AI4</td>
<td>• • • • •</td>
</tr>
<tr>
<td>4. Install and accredit solutions and changes.</td>
<td>AI7</td>
<td>• • • • •</td>
</tr>
<tr>
<td>5. Manage changes.</td>
<td>AI6</td>
<td>• • • •</td>
</tr>
<tr>
<td>6. Define and manage service levels.</td>
<td>DS1</td>
<td>• • • • •</td>
</tr>
<tr>
<td>7. Manage third-party services.</td>
<td>DS2</td>
<td>• • • • •</td>
</tr>
<tr>
<td>8. Ensure systems security.</td>
<td>DS5</td>
<td>• • •</td>
</tr>
<tr>
<td>9. Manage the configuration.</td>
<td>DS9</td>
<td>• • • •</td>
</tr>
<tr>
<td>10. Manage problems and incidents.</td>
<td>DS8, DS10</td>
<td>• • • • • •</td>
</tr>
<tr>
<td>11. Manage data.</td>
<td>DS11</td>
<td>• • • • •</td>
</tr>
<tr>
<td>12. Manage the physical environment and operations.</td>
<td>DS12, DS13</td>
<td>• • • • •</td>
</tr>
</tbody>
</table>
Scoping the IT Control Project

ITIL PROCESSES
- Service Level Management
- Incident Management
- Change Management
- Release Management
## Target range of Internal Control

<table>
<thead>
<tr>
<th>Targeted Business Processes</th>
<th>US/Canada</th>
<th>Japan</th>
<th>UK</th>
<th>Italy</th>
<th>Germany</th>
<th>Holland</th>
<th>France</th>
<th>Brazil</th>
<th>Australia</th>
<th>Switzerland</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Fixed Assets</td>
<td>P</td>
<td>V</td>
<td>P</td>
<td>P</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>2. Tax</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>V</td>
</tr>
<tr>
<td>5. Payroll</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>6. HR</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>8. Indirect Sales</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>11. Capitalized Software</td>
<td>P</td>
<td>N/A</td>
<td>P</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>12. IT</strong></td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>V</td>
</tr>
<tr>
<td>13. Swiss Cash Pooling</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>P</td>
</tr>
</tbody>
</table>

- **P**: In Scope
- **V**: Not in scope
- **P**: In Scope for External Auditor – However, External Auditor will review all documentation
It is required that executive management to attest quarterly that reasonable and prudent controls are in place to provide accurate and complete financial management reports.

The Attestation of Controls occurs at 3 Key Levels

- Business Controls
- Application Controls
- IT Process Controls
**COBIT – providing extensive IT Governance material**

- **Business Goals**
  - Requirements
  - Information
- **IT Processes**
  - Goals
  - Key Activities
  - Control Outcome Tests
  - Control Objectives
  - Control Practices
- **Maturity Models**
  - Performance Indicators
  - Outcome Measures
  - Maturity Models
- **Responsibility & Accountability Chart**
  - Performed by
  - Baseline on
- **Control Design Tests**
  - Audited with
  - Implemented with
COBIT: An IT governance framework

- **Domain**
- **Process Name**
- **Process Description**
- **Maturity Model**

**IT PROCESS**

- **Process Goals**
- **Key Activity**
- **RACI chart**
- **Inputs**
- **Outputs**
- **Goal Metric**
- **Activity Goal**
- **Activity Metric**
- **TO IT Process**
- **FROM IT Process**

**IT Goals**

**Themes**

- **Control Objective**
  - **Value Statements**
  - **Risk Statements**
  - **Control Practices**

- **ASSURANCE STEPS**
  - Control Design & Operation
  - Control Objective Outcome
  - Control Weakness Impact
IT Control Practices

- A non-prescriptive control design for achieving the control objective
- Describing the different necessary and sufficient steps to achieve a control objective
- Action-oriented, enabling timely execution and measurable
- Relevant to the purpose of the control objective
- Covering all inputs, activities and outputs of the process
- Supporting clear roles and responsibility including segregation
- Concepts of active and passive components
- Generic and specific practices
IT Assurance Steps

• Testing of a control approach covering 4 assurance objectives
  – Existence
  – Design effectiveness
  – Operating effectiveness (implemented, consistent application and proper use)
  – Design and operating efficiency (cost/benefit and possible use of automation)

• Providing 3 types of assurance guidance
  – Testing the suggested control design
  – Testing control objective achievement
  – Documenting impact of control weaknesses

• Tests based on a documented taxonomy of relevant assurance methods
  – Enquire and confirm (via different source)
  – Inspect (walk-through, search, compare, review)
  – Observe (confirmation is inherent)
  – Re-perform or re-calculate and analyse (often based on a sample)
  – Automated evidence collection (sample, trace, extract) and analyse
## IT Control Practices and Assurance Steps

### PO6 Communicate Management Aims and Direction

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Value Drivers</th>
<th>Risk Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO6.2 Enterprise IT Risk and Control Framework</strong></td>
<td>• Comprehensive IT control and risk framework</td>
<td>• Sensitive corporate information is disclosed</td>
</tr>
<tr>
<td>Develop and maintain a framework that defines the enterprise’s overall approach</td>
<td>• IT risks and control awareness and understanding</td>
<td>• No identification of irregularities</td>
</tr>
<tr>
<td>to IT risk and control that aligns with the IT policy and control environment and</td>
<td></td>
<td>• Financial losses</td>
</tr>
<tr>
<td>the enterprise risk and control framework.</td>
<td></td>
<td>• Compliance and security issues</td>
</tr>
</tbody>
</table>

### Control Practices

1. Define an IT risk and control framework adopting relevant guidance such as COSO Internal Control – Integrated Framework, COSO Enterprise Risk Management – Integrated Framework and COBIT.
2. The enterprise IT risk and control framework specifies:
   - Purpose of the internal control framework
   - Scope of the control framework (i.e., IT process framework)
   - Management’s expectation of what needs to be controlled and roles and responsibilities
   - Methodologies to be used
3. Ensure the aim at maximising success of value delivery while minimising risks to information assets through preventive measures, timely identification of irregularities, limitation of losses and timely recovery of business assets.

### PO6 Communicate Management Aims and Direction

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Value Drivers</th>
<th>Risk Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PO6.2 Enterprise IT Risk and Control Framework</strong></td>
<td>• Comprehensive IT control and risk framework</td>
<td>• Sensitive corporate information is disclosed</td>
</tr>
<tr>
<td>Develop and maintain a framework that defines the enterprise’s overall approach</td>
<td>• IT risks and control awareness and understanding</td>
<td>• No identification of irregularities</td>
</tr>
<tr>
<td>to IT risk and control that aligns with the IT policy and control environment and</td>
<td></td>
<td>• Financial losses</td>
</tr>
<tr>
<td>the enterprise risk and control framework.</td>
<td></td>
<td>• Compliance and security issues</td>
</tr>
</tbody>
</table>

### Testing the Control Design

Enquire and confirm that a formal IT risk and control framework exists based on acknowledged industry leading practices (e.g. COSO and COBIT). Assess whether the IT risk and control framework is aligned with the organization’s risk and control framework and considers the enterprise risk tolerance level. Enquire and confirm that the IT risk and control framework specifies its scope and purpose and outlines management’s expectations of what needs to be controlled. Enquire and confirm that the structure of the IT risk and control framework is well defined and responsibilities have been clearly stated and assigned to appropriate individuals. Enquire and confirm that a process is in place to periodically review (recommend annual reviews) the IT risk and control framework to maintain its adequacy and relevancy.
Example 1
COBIT and ITIL

- Large Global Bank
- Implementing ITIL and have multiple compliance frameworks
- Using COBIT for Governance, Audit, SOX and JSOX
- ITIL implementation required parameters, metrics and validation
- Control practices aligned to metrics from the ITIL processes
Example 1
COBIT and ITIL

COBIT
AI6.1 Change Standards and
AI6.3 Emergency Changes
AI6.4 Change Status Tracking and Reporting
AI6.5 Change Closure and Documentation

ITIL
Request for changes (RFCs)
Change Advisory Board
IT services (SLAs)

- Control
- Monitoring or performance

Automation of recording changes using a tool for automated change management software

- Activity Goals measuring the ITIL processes
  - Develop and implement a process to consistently record, assess and prioritise change requests.
  - Assess impact and prioritise changes based on business needs.
  - Assure that any emergency and critical change follows the approved process.
  - Authorise changes
  - Manage and disseminate relevant information regarding changes
Example 2
COBIT and ITIL

• Health Care Provider
• Started implementing ITIL and halted pending Governance
• Using COBIT for Governance, Audit, SOX and JSOX
• Service Levels– failure to deliver a risk to revenue
• Control practices aligned to metrics from the ITIL processes
Example 2
COBIT and ITIL

COBIT
DS1.1 Service Level Management Framework
DS1.2 Definition of Services
DS1.3 Service Level Agreements
DS1.4 Operating Level Agreements
DS1.5 Monitoring and Reporting of Service Level Achievements
DS1.6 Review of Service Level Agreements and Contracts

Activity Goals
• Create a framework for defining IT services.
• Build an IT service catalogue. Define service level agreements (SLAs) for critical IT services.
• Define operating level agreements (OLAs) for meeting SLAs.
• Monitor and report end-to-end service level performance.
• Review SLAs and underpinning contracts.
• Review and update IT service catalogue.

ITIL
IT services (SLAs)
IT service catalogue

• Control
• Monitoring or performance

Automation the recording of service levels
Definition and use of a service catalogue
Agenda

• Frameworks
  – COBIT
  – ITIL
  – ISO/IEC 20000
• USING COBIT with ITIL
• Practical experience
• **Summary**
Implications for IT Professionals

- Develop solid understanding of control theory
  - General controls
  - Automated application controls
- Develop and incorporate an ongoing risk assessment process into IT management activities
- Develop and implement new controls for new risks identified in risk assessment process
- Develop and maintain documentation of controls performed within the IS environment
- Continuously assess design of controls in changing IS environments
- Learn how to test the operating effectiveness of controls with the IS environment and conduct annual tests of key controls
- Develop and maintain evidence of tests of controls
- Automate
- Use Change Management
Compliance = Competitive Advantage

- Enhance overall IT governance
- Enhance the understanding of IT among executives
- Aid better business decisions
- Align project initiatives with business requirements
- Prevent loss of intellectual assets and the possibility of system breach
- Contribute to the compliance of other regulatory requirements
- Realize more efficient and effective operations
- Optimize operations
- Enhance risk management competencies
IT Governance Institute is a non-profit research think-tank run by ISACA
www.isaca.org
www.itgi.org
COBIT & ITIL usage for SOX - current and future

Robert E Stroud
International Vice President ISACA
Evangelist ITSM & IT Governance CA, Inc.

Japan, November 8, 2007