Integrating COBIT® into the IT Audit Process (Planning, Scope Development, Practices)

April 20, 2006
San Francisco ISACA Chapter Luncheon Seminar

Presented By
Lance M. Turcato, CISA, CISM, CPA
Deputy City Auditor – Information Technology
City of Phoenix
Audience Poll

**COBIT Knowledge**

- First exposure?
- General understanding?
- Strong knowledge of COBIT framework?

**Current Users of COBIT**

- Incorporated Into Audit Process?
- Adopted by IT Management?
- Users of a framework other than COBIT?
<table>
<thead>
<tr>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of COBIT® Components</td>
</tr>
<tr>
<td>Integrating COBIT® Domains into IT Audit Planning &amp; Scope Development</td>
</tr>
<tr>
<td>- Audit Universe Considerations</td>
</tr>
<tr>
<td>- Ensuring Consistent Coverage</td>
</tr>
<tr>
<td>- Integrating Relevant Industry Standards, Guidelines, and Best Practices</td>
</tr>
<tr>
<td>- Organizational IT Policy, Standard, Guideline, and Procedure Considerations</td>
</tr>
<tr>
<td>Integrating COBIT® into the IT Audit Lifecycle</td>
</tr>
<tr>
<td>Using COBIT® to Establish IT Risk &amp; Control Measurement</td>
</tr>
<tr>
<td>Resources &amp; Wrap-up</td>
</tr>
</tbody>
</table>
Overview of COBIT® Components

IT Governance Institute
(http://www.itgi.org/ )
**CobiT® - Background**

“Generally applicable and accepted international standard of good practice for IT control”

**C**ontrol **O**bjectives for **I**nformation and Related **T**echnology

“An authoritative, up-to-date, international set of generally accepted *Information Technology Control Objectives* for day-to-day use by business managers and auditors.”
**COBIT’s Scope & Objectives**

- **COBIT® 4.0** was developed and by the IT Governance Institute ([www.itgi.org](http://www.itgi.org)) and was released in December, 2005.

- **COBIT®** has evolved into an IT governance / control framework:
  - A toolkit of “best practices” for IT control representing the consensus of experts
  - IT Governance focus
  - Linkage with business requirements (bridges the gap between control requirements, technical issues, and business risks).
  - Management – process owner – orientation (accountability)
  - Measurement and maturity driven
  - Generic focus – applicable to multiple environments
  - Organizes IT activities into a generally accepted process model (in alignment with ITIL, ISO, and other relevant ‘best practices’)
  - Identifies the major IT resources to be leveraged
  - Defines control objectives and associated assurance guidelines
COBIT® As A Framework

- Enables the **auditor** to review specific IT processes against COBIT’s Control Objectives to determine where controls are sufficient or advise management where processes need to be improved.

- Helps **process owners** answer questions - “Is what I’m doing adequate and in line with best practices? If not, what should I be doing and where should I focus my efforts?”

- COBIT® is a **framework** and is **NOT** exhaustive or definitive. The scope and breadth of a COBIT® implementation varies from organization to organization.

- COBIT® prescribes “what” best practices should be in place. An effective implementation requires that COBIT® be supplemented with other sources of best practice that prescribe the “how” for IT governance and controlled process execution.
Hierarchy of COBIT® Components

“The Method Is...”

“The Minimum Controls Are...”

“How You Measure Your Performance ...”

“How You Implement...”

“How You Audit...”

“The COBIT Framework*”

“IT Assurance Guide”

“IT Control Objectives for Sarbanes-Oxley”

“COBIT Quickstart”

“COBIT Security Baseline”

* Now integrated into COBIT 4.0
Relationship of COBIT® Components
CobIT® Structure

Overview

- Starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives
- Promotes process focus and process ownership
- Divides IT into 34 processes belonging to four domains (providing a high level control objective for each process)
- Looks at fiduciary, quality and security needs of enterprises, providing seven information criteria that can be used to generically define what the business requires from IT
- Is supported by a set of over 200 detailed control objectives

IT Domains
- Plan & Organize
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate

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

Business Requirements
CobiT® Structure
Aligning Requirements, Processes, Resources & Activities

- Natural grouping of processes, often matching an organizational domain of responsibility.
- A series of joined activities with natural (control) breaks.
- Actions needed to achieve a measurable result. Activities have a life-cycle whereas tasks are discreet.
CobiT® Structure
Example

IT Domains
- Plan & Organize
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate

IT Processes
- Change Management
- Contingency Planning
- Problem Management
- Policy & Procedures
- Acceptance Testing
- etc...

Activities
- Record new problem
- Analyze problem
- Propose solution
- Monitor solution
- Record known problem
- etc...
CobIT® *High-Level Processes / Objectives*

**Plan & Organize**

- **PO 1** Define a Strategic IT Plan
- **PO 2** Define the Information Architecture
- **PO 3** Determine Technological Direction
- **PO 4** Define the IT Processes, Organization, & Relationships
- **PO 5** Manage the IT Investment
- **PO 6** Communicate Management Aims and Direction
- **PO 7** Manage IT Human Resources
- **PO 8** Manage Quality
- **PO 9** Assess & Manage IT Risks
- **PO 10** Manage Projects
C OB IT® High-Level Processes / Objectives

Acquire & Implement

AI 1 Identify Automated Solutions
AI 2 Acquire and Maintain Application Software
AI 3 Acquire and Maintain Technology Infrastructure
AI 4 Enable Operation and Use
AI 5 Procure IT Resources
AI 6 Manage Changes
AI 7 Install and Accredit Solutions and Changes
**CobiT® High-Level Processes / Objectives**

**Deliver & Support**

DS 1  Define and Manage Service Levels  
DS 2  Manage Third-Party Services  
DS 3  Manage Performance and Capacity  
DS 4  Ensure Continuous Service  
DS 5  Ensure Systems Security  
DS 6  Identify and Allocate Costs  
DS 7  Educate and Train Users  
DS 8  Manage Service Desk and Incidents  
DS 9  Manage the Configuration  
DS 10 Manage Problems  
DS 11 Manage Data  
DS 12 Manage the Physical Environment  
DS 13 Manage Operations
CobiT® High-Level Processes / Objectives

Monitor & Evaluate

M 1  Monitor and Evaluate IT Performance
M 2  Monitor and Evaluate Internal Control
M 3  Ensure Regulatory Compliance
M 4  Provide IT Governance
Linking The Processes To Control Objectives
(34 High-level and 200+ Detailed Objectives)

**CobIT’s Waterfall and Navigation Aids**

Linking *Process, Resource & Criteria*

*Image of diagram*

- **Information Criteria**
  - Effectiveness
  - Efficiency
  - Confidentiality
  - Integrity
  - Availability
  - Compliance
  - Reliability

- **The control of IT Process**
  - Business Requirements
  - IT Goals
  - Key Controls
  - Key Metrics

- **Process Domains**
  - Plan & Organize
  - Acquire & Implement
  - Deliver & Support
  - Monitor & Evaluate

*Image of diagram*
Example of COBIT® 4.0 - DS5 (page 1)

Deliver and Support
Ensure Systems Security

High-level Control Objective

DS5 Ensure Systems Security

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents.

Process Description

IT Domains & Information Indicators

IT Goals

Process Goals

Key Practices

Key Metrics

IT Governance & IT Resource Indicators
### Detailed Control Objectives

#### DSS Ensure Systems Security

<table>
<thead>
<tr>
<th>DSS 5.1 Management of IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage IT security at the highest appropriate organizational level, so the management of security actions is in line with business requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.2 IT Security Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translate business information requirements, IT configuration, information risk action plans and information security culture into an overall IT security plan. The plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Security policies and procedures are communicated to stakeholders and users.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.3 Identity Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository. Countermeasures technical and procedural measures are deployed to prevent and detect to establish user identification, implement authentication and enforce access rights.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.4 User Access Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure ensuring the data of system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Performance regular management review of all accounts and related privileges.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.5 Security Testing, Surveillance and Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that IT security implementation is tested and monitored proactively. IT security should be re-audited periodically to ensure the approved security level is maintained. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. Access to the logging information is in line with business requirements in terms of access rights and retention requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.6 Security Incident Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the definitions of potential security incidents are clearly defined and communicated so security incidents can be properly treated by the incident or problem management process. Characteristics include a description of what is considered a security incident and its impact level. A limited number of impact levels are defined and for each the specific actions required and the people who need to be notified are identified.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.7 Protection of Security Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that important security-related technology is made resistant to tampering and security documentation is not disclosed unnecessarily, i.e., keeps a low profile. However, do not make security of systems reliant on secrecy of security specifications.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.8 Cryptographic Key Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine policies and procedures to organize the generation, change, revocation, destruction, distribution, certification, storage, entry use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.9 Malicious Software Prevention, Detection and Correction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that preventive, detective and corrective measures are in place especially up-to-date security patches and virus control across the organization to protect information systems and technology from malware (viruses, worms, spyware, spam, internally developed malicious software, etc.).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.10 Network Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) are used to monitor access and control information flows from and to networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS 5.11 Exchange of Sensitive Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that sensitive transaction data is exchanged only over a trusted path or medium with controls to provide authenticity of content, proof of transmission, proof of receipt and non-repudiation of origin.</td>
</tr>
</tbody>
</table>
CobIT® Management Guidelines

CobIT 3rd Edition added a Management and Governance layer, providing management with a toolbox containing...

- A maturity model to assist in benchmarking and decision-making for control over IT
- A list of critical success factors (CSF) that provides succinct non-technical best practices for each IT process
- Generic and action oriented performance measurement elements (key performance indicators [KPI] and key goal indicators [KGI] - outcome measures and performance drivers for all IT processes)

Purpose...
- IT Control profiling – what is important?
- Awareness – where is the risk?
- Benchmarking - what do others do?
Maturity Model: Method of scoring the maturity of IT processes…

LEGEND FOR SYMBOLS USED
- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED
0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.
Metrics as CSF, KPI, & KGI

- **Critical Success Factors (CSF)**
  What are the most important things to do to increase the probability of success of the process?

- **Key Performance Indicators (KPI)**
  Measure how well a process is performing.

- **Key Goal Indicators (KGI)**
  Measure whether a process achieved its business requirements.
Measuring Success – Example of CoBIT® DS5

Define goals.

Activity Goal
- Understand security requirements, vulnerabilities and threats.
  - is measured by Frequency of review of the type of security events to be monitored.

Process Goal
- Detect and resolve unauthorised access to information, applications and infrastructure.
  - is measured by Number of access violations.

IT Goal
- Ensure IT services can resist and recover from attacks.
  - is measured by Number of actual IT incidents with business impact.

Business Goal
- Maintain enterprise reputation and leadership.
  - is measured by Number of incidents causing public embarrassment.

Measure achievement.

Drive performance.

KPI Business Metric KGI
KPI IT Metric KGI
KPI Process Metric KGI

Improve and realign.
Example of COBIT® 4.0 - DS5 (page 3)

Process Relationships

RACI Chart
(Major activities and associated responsibilities)

IT Goals & Performance Metrics
Example of COBIT® 4.0 - DS5 (page 4)

Maturity Model

DS5 Ensure Systems Security

Management of the process of ensuring systems security that satisfies the business requirements for IT of maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents is:

0. Non-existent when
The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognisable system security administration process.

1. Initial/Ad Hoc when
The organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2. Repeateable but Intuitive when
Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is inadequate, misleading or not present. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see that IT security is within its domain.

3. Defined Process when
Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. Ad hoc security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business but is only informally scheduled and managed.

4. Managed and Measurable when
Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Exposure to threats for promoting security awareness is mandatory. User identification, authorisation and authorisation are standardised. Security certification is pursued for staff who are responsible for the audit and management of security. Security testing is done using standard and formalised processes leading to improvements of security levels. IT security processes are co-ordinated with an overall organisation security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. KPIs and KPIs for security management have been defined but are not yet measured.

5. Optimised when
IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analysed. Adequate controls to mitigate risk are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organisationwide. KPIs and KPIs for security management are collected and communicated. Management uses KPIs to adjust the security plan in a continuous improvement process.
Summing It All Up

Business Goals Drive IT Goals

[Diagram showing the relationship between business goals, governance drivers, business outcomes, IT processes, and IT goals.]

- Business Goals
  - Governance Drivers
  - Business Outcomes
  - Information Criteria
  - IT Resources
  - Key Performance Indicators
  - Key Goal Indicators
  - High-level Control Objectives

- IT Processes
  - Applications
  - Information
  - Infrastructure
  - People
Integrating COBIT® Domains Into IT Audit Planning & Scope Development
Integration Overview

- Map COBIT to the Technology Audit Universe
- Ensure Consistent Audit Coverage By Establishing IT Audit Focal Points
- Integrate COBIT Into the IT Audit Lifecycle
  - Map COBIT to the Annual and Rotational Audit Plans
  - Develop Work Programs (Supplement Existing Work Programs With COBIT Audit Guidelines)
  - Joint Risk Self-Assessments
  - Analyze, Document, Validate Results
  - Report To Management
- Use COBIT To Establish IT Risk & Control Measurement
Mapping COBIT® to the Technology Audit Universe
Drilling Down to the Technology Infrastructure

- Division / Business
- Business Cycles
- Applications
- Operating System / Platform

Financial Statement Accounts
- Financial Accounting
- Fixed Assets
- Expenditures
- Inventory
- Revenue
- Payroll

Understand / Assess Risk

- SAP
- Various Others

- UNIX
- Various Other Systems
Identifying Relevant Technology “Layers”

INFORMATION TECHNOLOGY POLICIES & STANDARDS

IT Procedures (document how to implement security standards / requirements)

Administration Tools

Distributed Applications

Mainframe Applications

Distributed Databases

Oracle DB2 Sybase SQL/Server

Mainframe Databases

DB2 Datacom

Distributed Servers

Windows NT / 2000 / XP UNIX

Mainframes

MVS (OS/390), TopSecret, RACF

Firewall Components (Routers, Bastion Hosts & Firewall Applications)

Other Network Components

Monitoring & Incident Response

April 20, 2006
SF ISACA - April Chapter Luncheon
Understanding the IT Governance Framework

IT Governance
- IT Risk Management
- Oversight
- IT & Business Alignment

IT Strategy & Planning
- IT Planning
- Strategic Sourcing
- IT Organization
- Budget & Control

IT Management
- Change Management
- Project Management
- Quality Assurance
- Portfolio Management

Program Management
- Technology Management
  - Technology Planning
  - Architecture Design
  - Vendor / Product Selection
- Operations
  - Data Center Operations
  - Storage Management
  - Data Management
  - Network & Systems Mgt
  - Desktop Management
  - Release Management
  - Performance Management
- Applications
  - Development
    - Testing
    - Conversion
    - Implementation
  - IT Change Management
  - Maintenance
- Support
  - Vendors / 3rd Party
  - Help Desk
  - End User Support
  - Training

Enterprise Security Architecture & Management

Disaster Recovery Planning

IT Human Resources
Defining the Technology Audit Universe

Audit Universe

Data Center Operations

User Support

Recoverability

Performance & Capacity

Architecture

Hardware Management

Software Management

System Development

Database Management

Problem Management

Change Management

Telecommunications

Network Management

Information Security

- Distributed Servers
- Mainframe
- Distributed & Mainframe Databases
- Information Privacy
- Monitoring & Intrusion Detection
- Physical Security

- Network & Perimeter
- Remote Access
- Security Engineering
- Security Management
- Virus Prevention
- Applications

Defining the Technology Audit Universe
Security Audit Universe

Mainframe Security
- O/S (OS/390)
- Security Systems (Top Secret / RACF)
- Sub-systems (CICS, TSO, IMS DC, MQ)
- Mainframe Databases (DB2, Datacom)

Distributed Server Security
- UNIX (Solaris, AIX, HP-UX)
- Windows NT / 2000 / XP
- Netware

Distributed Database Security
- DB2 6000
- Oracle
- SQL/Server
- Sybase

Information Privacy
- Privacy Office Compliance Program

Virus Prevention
- Anti-Virus Program

Security Management
- Policy, Standards, & Procedures Maintenance Process
- Security Awareness Program
- Security Metrics & Performance Reporting

Security Engineering
- Research & Development
- Security Self-Assessments

Network & Perimeter Security
- Firewalls
- Subsidiary Connectivity
- 3rd Party Connectivity

Remote Access Security
- VPNs
- Modem Usage
- Other Remote Access Facilities
- Vendor Access

Monitoring & Incident Response
- System Logging & Reporting
- Automated Intrusion Detection Systems (IDS)
- Vulnerability Assessment Process
- Incident Response Program

Application Security
- ETS Audit Coverage
- System Development Projects

Physical Security

April 20, 2006
**High Level Objective (e.g. PO2)**

### Map Audit Universe To COBIT®

<table>
<thead>
<tr>
<th>Ref.</th>
<th>COBIT Domains &amp; High-Level Control Objectives</th>
<th>Infrastructure Audit Universe</th>
<th>Security Audit Universe</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>PLANNING &amp; ORGANIZATION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F01</td>
<td>Define a Strategic IT Plan</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>F02</td>
<td>Define the Information Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F03</td>
<td>Establish the Technological Direction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F04</td>
<td>Define the IT Organization and Relationships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F05</td>
<td>Manage the Information Technology Investment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F06</td>
<td>Communication Management Policy and Practice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F07</td>
<td>Manage Human Resources</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>F08</td>
<td>Ensure Compliance with External Requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F09</td>
<td>Access Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F10</td>
<td>Manage Projects</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>F11</td>
<td>Acquire and Maintain High-Level Control</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Objectives Noted With ‘X’**

**Illustration Only**
Ensuring Consistent Coverage

*IT Audit Focal Points*
Audit Focal Points

ensure consistent coverage across audits and allow for trending the “state of controls” over time.

Infrastructure

- Strategy & Structure
- Methodologies & Procedures
- Measurement & Reporting
- Tools & Technology

Information Security

- Access Control
- System Security Configuration
- Monitoring, Vulnerability Assessment, & Response
- Security Management & Administration

Example
Standards & Procedures
- Standards and procedures for access control are documented, approved, and communicated.

Account Management
- Account management procedures exist and are effective.

Password Management
- Password management mechanisms are in place to ensure that user passwords comply with Schwab password syntax and management criteria.

User Profile Configurations
- User profile configurations are defined based on job responsibilities.

Group Profile Configurations
- Group profile configurations are defined to ensure consistent access by users performing similar job responsibilities.

Privileged & Special User Accounts
- Privileged and Special User accounts are authorized and restricted.

Generic & Shared Accounts
- Generic & Shared accounts are not used as per Schwab standards.

Logon / Logoff Processes
- Systems should be configured to lock after consecutive invalid attempts.

System Boot Process
- System boot process is configured to ensure that only authorized security settings and system services are initiated during the system boot / IPL process.

Remote Access
- Appropriate mechanisms are in place to control and monitor remote user access to Schwab's internal network.

Resource Safeguards (File/Dataset & Directory/Volume Protection)
- System level security has been configured to appropriately protect critical system resources (files/datasets, directories/volumes, applications, etc.).

Security Program Strategy
- Overall security strategy and direction has been established and communicated.

Security Policy & Standards
- Overall security policy and standards are documented, approved and communicated.

Procedures
- Daily operational procedures have been defined, documented and communicated to ensure that individuals with administrative responsibilities are able to effectively execute standard administration procedures.

Roles, Responsibilities, & Staffing
- Roles and responsibilities have been defined, documented and communicated to ensure that individuals are informed of their responsibilities.

User Education & Awareness
- Awareness and education programs have been established to ensure that users are aware of appropriate corporate security policy and standards.

Security Advisories & Alerts
- Industry security advisories and alerts should be closely monitored to ensure that appropriate mitigating controls are in place for identified vulnerabilities / exposures.

Security Administration
- Responsibility for security administration is appropriately assigned and accountability has been established.

Environment Understanding
- Gain a comprehensive understanding of the computer-processing environment and the relevant controls in place.
Map Focal Points / Areas of Emphasis to COBIT®

(Example)

**Access Control**

**Standards & Procedures**
- Standards and procedures for access control are documented, approved, and communicated.

**Account Management**
- Account management procedures exist and are effective.

**Password Management**
- Password management mechanisms are in place to ensure that user passwords comply with Schwab password syntax and management criteria.

**User Profile Configurations**
- User profile configurations are defined based on job responsibilities.

**Group Profile Configurations**
- Group profile configurations are defined to ensure consistent access by users performing similar job responsibilities.

**Privileged & Special User Accounts**
- Privileged and Special User accounts are authorized and restricted.

**Generic & Shared Accounts**
- Generic & Shared accounts are not used as per Schwab standards.

**Logon / Logoff Processes**
- Systems should be configured to lock after consecutive invalid attempts.

**System Boot Process**
- System boot process is configured to ensure that only authorized security settings and system services are initiated during the system boot / IPL process.

**Remote Access**
- Appropriate mechanisms are in place to control and monitor remote user access to Schwab's internal network.

**Resource Safeguards (File/Dataset & Directory/Volume Protection)**
- System level security has been configured to appropriately protect critical system resources (files/datasets, directories/volumes, applications, etc.).

SF ISACA - April Chapter Luncheon

April 20, 2006
Mapping COBIT® to Relevant Industry Standards, Guidelines & Best Practices

Vendor-Specific Guidance
Classifying Sources

Identify relevant industry standards, guidelines, and best practices (classify by purpose)...

- Governance (strategic) focus versus Management (tactical) focus.

- Process Control focus versus process Execution focus.

- What To Do versus How To Do IT
Classification (Example)

**GOVERN**
- Strategic
- Control

**MANAGE**
- Tactical
- Execute

ISO17799

Vendor-Specific Guidance
ITIL Overview

- Information Technology Infrastructure Library (ITIL)
- Set of books detailing best practices for IT Service Management (the “how”)
- Originally developed by the UK government to improve IT Service Management
- Now more globally accepted
- Currently under revision

www.itil.co.uk
ITIL – The Most Popular Books

Service Support

Service Desk

Service Delivery

- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management
- Service Level Management
- Capacity Management
- Availability Management
- Service Continuity Management
- Financial Management

Source: 2005 COBIT User Convention
ITIL Mapping To COBIT®
(continued)

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

Source: 2005 COBIT User Convention
ISO 17799 Overview

- ISO/IEC 17799:2005
  *Code of Practice for Information Security Management*
- Established guidelines and general principles for initiating, implementing, maintaining, and improving information security management.
- Objectives outlined provide general guidance on the commonly accepted goals of information security management.
- Updated in 2005
- [www.iso.org](http://www.iso.org)
ISO 17799 contains best practices for control objectives and controls in the following areas…

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical & Environmental Security
- Communications & Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance
Aligning COBIT®, ITIL, and ISO 17799

A Management Briefing from ITGI and OGC…

➢ IT Governance Institute
➢ Office of Government Commerce.
➢ Useful guidance for implementing COBIT, ITIL and ISO17799
➢ Useful mapping of ITIL and ISO17799 to COBIT (3rd edition)
➢ Available at ISACA.ORG
  ▪ Go to Downloads
  ▪ Then COBIT
Mapping COBIT® to Organizational IT Policies, Standards, Guidelines & Procedures
Policies, Standards, Guidelines & Procedures

**IT Policies**
- **Policies:**
  High-level statements. When there is no specific standard to follow, policies provide general guidance.

**IT Standards**
- **Standards:**
  Standards establish a point of reference, providing criteria that may be used to measure the accuracy and effectiveness of procedures/mechanisms that are in place.

**IT Guidelines**
- **Guidelines:**
  Guidelines provide specific and detailed requirements relative to implementing specific IT standards (i.e., platform specific; function specific; component specific, etc.).

**IT Procedures**
- **Procedures:**
  Procedures provide step-by-step instructions for end-users and technical staff for the execution of specific IT processes.
Map COBIT® To IT Policies, Standards, Guidelines & Procedures

<table>
<thead>
<tr>
<th>High Level Objective</th>
<th>Detailed Level Objective</th>
<th>IT Policies</th>
<th>IT Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e.g. PO1)</td>
<td>(e.g. 2.1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Objectives Noted**
Integrating COBIT® Into the IT Audit Lifecycle
IT Audit Approach Overview

COBIT Manuals & Other Best Practice Material

Audit Planning Session

Audit Team

COBIT Risk & Control Assessment Questionnaire

Audit Testing

Exit Meeting

Reporting

QAR

Engagement Scope

Kick-Off Meeting

Work Program

Client Work Sessions

COBIT To Audit Mapping Template

Planning & Scheduling

Risk & Control Assessment

Audit Reporting

CobiT To Audit Mapping Template

CobiT Risk & Control Assessment Questionnaire
### Map Audit Scope To COBIT®

#### COBIT Integration

**COBIT To Audit Mapping Template**

<table>
<thead>
<tr>
<th>Ref.</th>
<th>COBIT Domains &amp; Control Objectives</th>
<th>Applicable COBIT Control Objectives (mark with 'X')</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PLANNING &amp; ORGANIZATION</td>
</tr>
<tr>
<td>P01</td>
<td>Define a Strategic IT Plan</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>IT as Part of the Organization’s Long- and Short-Range Plan</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>IT Long-Range Plan</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>IT Long-Range Planning, Approach &amp; Structure</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>IT Long-Range Plan Changes</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Short-Range Planning for the IT Function</td>
<td></td>
</tr>
<tr>
<td>1.6</td>
<td>Communication of IT Plans</td>
<td></td>
</tr>
<tr>
<td>1.7</td>
<td>Monitoring &amp; Evaluating of IT Plans</td>
<td></td>
</tr>
<tr>
<td>1.8</td>
<td>Assessment of Existing Systems</td>
<td></td>
</tr>
</tbody>
</table>

#### Detailed Level Objective (e.g. 2.1)

- 2.1 Information Architecture Model
- 2.2 Corporate Data Dictionary & Data Syntax Rules
- 2.3 Data Classification Scheme
- 2.4 Security Levels

#### High Level Objective (e.g. P01)

#### P02 Define the Information Architecture

- 2.1 Information Architecture Model
- 2.2 Corporate Data Dictionary & Data Syntax Rules
- 2.3 Data Classification Scheme
- 2.4 Security Levels

#### P03 Determine Technological Direction

- 3.1 Technological Infrastructure Planning
- 3.2 Monitor Future Trends & Regulations
- 3.3 Technological Infrastructure Contingency
- 3.4 Hardware and Software Acquisition Plan
- 3.5 Technology Standards

#### P04 Define the IT Organization and Relationships

- 4.1 IT Planning or Steering Committee
- 4.2 Organizational Placement of the IT Function
- 4.3 Review of Organizational Achievements
- 4.4 Roles & Responsibilities

Supplemented by other mapping results…

---

*April 20, 2006*
Using COBIT® Framework To Tie It All Together…

Audit Scope Memo Defined

Use of a Framework ensures consistent coverage across audits and allows for trending the “state of controls” over time.
CobiT® Control Assessment Questionnaire

Questionnaire is used during joint work sessions held with clients to complete a joint risk assessment of the area under review.

<table>
<thead>
<tr>
<th>High-level Control Objective</th>
<th>Overall Maturity Rating</th>
<th>Detailed Control Objectives</th>
<th>Maturity Rating</th>
<th>Assessment Questions</th>
<th>Client Response &amp; Assessment Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-level Objective 1 (follow CobiT order: PO first, then AI, DS, M)</td>
<td>Overall Maturity Rating: (Insert Rating Here)</td>
<td>CobiT Maturity Rating (0-5) assigned based on Joint Assessment</td>
<td>Preplanned Assessment Questions</td>
<td>Client’s Response &amp; Assessment Results</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Visitor Record

Objectives Specific to XYZ Company Technology Area Under Review:

- Write visitor name on visitor badge; remove badge from the visitor after the visit.
- Visitor badge should be scanned on entry and exit of each visitor to the site.
- A visitor provided with an electronic access badge if, where possible, access to computer systems and sensitive areas should be controlled and monitored.
- Visitor access to control areas should be considered as appropriate IT guidelines.

Applicable CobiT Objective:

- A.1.3.3 Visitor Management

Applicable CobiT Objective: Specific to XYZ Company Technology Area Under Review

- XYZ Company specific objectives here

**Note of CobiT Detailed Objective:**

- Include XYZ Company specific objectives here
## COBIT® Based Executive Audit Report

### Executive Summary

<table>
<thead>
<tr>
<th>Overall Conclusion Statements</th>
<th>Supporting Overall Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concise Background &amp; Scope</td>
<td>MGT Reports</td>
</tr>
<tr>
<td>Control Weakness highlighting business impact</td>
<td>Responsible Manager Provided Response</td>
</tr>
<tr>
<td>Issue Priority (A, B, C)</td>
<td>Due Date</td>
</tr>
<tr>
<td>Overall Rating</td>
<td>Clients Target Goal</td>
</tr>
</tbody>
</table>

### Audit Metrics

<table>
<thead>
<tr>
<th>Responsible Manager Overall Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concise Background &amp; Scope</td>
</tr>
<tr>
<td>Control Weakness highlighting business impact</td>
</tr>
<tr>
<td>Issue Priority (A, B, C)</td>
</tr>
<tr>
<td>Overall Rating</td>
</tr>
</tbody>
</table>

### Clients Target Goal

<table>
<thead>
<tr>
<th>Client Provided Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT Reports</td>
</tr>
</tbody>
</table>

### Overall Rating

<table>
<thead>
<tr>
<th>Overall Conclusion Statements</th>
<th>Supporting Overall Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concise Background &amp; Scope</td>
<td>MGT Reports</td>
</tr>
<tr>
<td>Control Weakness highlighting business impact</td>
<td>Responsible Manager Provided Response</td>
</tr>
<tr>
<td>Issue Priority (A, B, C)</td>
<td>Due Date</td>
</tr>
<tr>
<td>Overall Rating</td>
<td>Clients Target Goal</td>
</tr>
</tbody>
</table>

---

*April 20, 2006 SF ISACA - April Chapter Luncheon Page 59*
CobIT® Based Audit Report (continued)

<table>
<thead>
<tr>
<th>Overall Rating</th>
<th>For High-Level Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Detailed Control Objectives Included In Scope Listed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applicable Detailed Control Objective (one per row; corresponds to a row in the Assessment Questionnaire)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assigned Maturity Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategic Focal Point Table (one row for each high-level objective included in scope)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Highlighting Key Performance Indicators (i.e., Metrics)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary Conclusions and Points Supporting Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Focal Point Table (highlighting key controls)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Highlighting Key Performance Indicators (i.e., Metrics)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary Conclusions and Points Supporting Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
### CobIT® Based Audit Report (continued)

**Process Workflow Diagram For Area Assessed**

**Table Defining Key Control Points In Process Flow**

**Highlighting Key Performance Indicators (i.e., Metrics)**

#### Process Workflow Diagram

![Process Workflow Diagram](image)

#### Table Defining Key Control Points In Process Flow

<table>
<thead>
<tr>
<th>Control Point</th>
<th>Summary Description</th>
<th>Control</th>
<th>Effect</th>
<th>Performance Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>Initiating process</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>X2</td>
<td>Process control</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>X3</td>
<td>Finalizing process</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>X4</td>
<td>Monitoring process</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

#### Automated or Manual Control

- **Automated Control**
- **Manual Control**
Using COBIT® to Establish IT Risk & Control Measurement
Goal is to proactively monitor audit results and IT metrics on an ongoing basis to focus the scope of audits on high-risk processes and tasks where performance indicators indicate potential problems.

Results of metric analysis is presented to client management on a periodic basis via management reports. The analysis indicates any changes to the audit scope planned for upcoming audits.
# COBIT® Measurement Repository

## Continuous Monitoring

## Questionnaire

## Audit Reports

---

### MGT Reports

**Trending Audit Results Over Time…**
Periodic Management Reports

Report to IT Management

Audit Results

&

Analysis of Key Technology Metrics

For the Quarter Ended

March 31, 2006

Audit Results Metrics

Analysis of Key Technology Metrics

Example of Metric Analysis To Include In QAR
(Illustration Only)

Although target rates have not been achieved, change management processes are successful on average 75% of the time. Less then 1% of appropriately recorded changes resulted in problems or outages...

Internal Audit Observations:

- Change management processes appear to be consistently applied with only minor variances in volume.
- Large percentage (>20%) of "unstatused" tickets indicate process adherence issues. True results cannot accurately be determined therefore, additional management scrutiny is appropriate for the "unstatused" items.
- Trend for tickets with implementation problems is increasing - additional analysis to ascertain root causes of this increase in this activity would be appropriate. Root cause may rest with testing and validation processes.
Example of Audit Result Metrics
(Illustration Only)

Legend:
- □ 5 - Optimized
- □ 4 - Managed
- □ 3 - Defined
- □ 2 - Repeatable
- □ 1 - Initial
- □ 0 - Non-Existent
Auditors monitor key indicators for mission critical technology functions on an ongoing basis…
Continuous Monitoring / Auditing
Ongoing Measurement / Ongoing Dialogue

Traditional Audit Approach
(Audit rotation schedule based on annual risk assessment of function)

“Point-In-Time” Audit – Challenges
- Evaluation of risk and control is as of a point in time.
- Audit reporting is reflective of results as of a point in time.
- Audit scope may be influenced by prior results.
- If an audit of the function has not been completed for a long time, there may be a learning curve.
Continuous Monitoring / Auditing
Ongoing Measurement / Ongoing Dialogue

Ongoing Monitoring Of Risk Indicators
(Gaining Efficiencies Through Focus On High Risk Indicators)

Benefits of Ongoing Monitoring
• Periodic (e.g., quarterly) readout of assessment results for technology management.
• Ongoing dialogue regarding areas of significant or increasing risk.
• IAD focuses the scope of individual audits on known risk factors ultimately leading to audit efficiencies which may result in less time impact on client personnel.
The Security Officer consistently performs both internal and external vulnerability scans on a monthly basis. The majority of vulnerabilities identified are low risk…

**Observations:**

- **A** An increase in *internal* vulnerabilities occurred from Q1 to Q2. The increase is explained due to new system patches checked for by the vulnerability scanner that have not been applied to the XYZ company servers. Technology management appropriately applies patches only after the patches have been tested and certified.

- **B** A decrease in *external* vulnerabilities was noted from Q1 to Q2. These results demonstrate that a significant number of Q1 vulnerabilities have been resolved.
Although target rates have not been achieved, change management processes are successful on average 75% of the time. Less than 1% of appropriately recorded changes resulted in problems or outages...

Internal Audit Observations:

- Change management processes appear to be consistently applied with only minor variances in volume.
- Large percentage (~20%) of “unstatused” tickets indicates process adherence issues. True results cannot accurately be determined; therefore, additional management scrutiny is appropriate for the “unstatused” items.
- Trend for tickets with implementation problems is increasing - additional analysis to ascertain root cause of the increase in this activity would be appropriate. Root cause may rest with testing and validation processes.
Summary & Wrap-Up
Benefits Realized…

- IT management partners with Internal Audit throughout the audit life cycle, including input into the audit schedule and scope.

- IT management becomes conversant in risk, control, and audit concepts.

- Relationships transformed into partnerships by jointly assessing control procedures.

- Audit Report streamlined…concise report supported by detailed questionnaire.

- Audit approach is methodical and is consistent with industry standards / best practices as well as IT Governance practices implemented throughout the company’s technology organization.

- Meaningful reporting for senior IT management.
Templates & Additional Resources

- Templates (www.sfisaca.org/resources/downloads.htm)
- IT Governance Implementation Guide (www.isaca.org)
- IT Control Practice Statements (www.isaca.org)
- Questionnaire for IT Control Practice Statements (www.isaca.org)
- IT Control Objectives for Sarbanes-Oxley (www.isaca.org)
- COBIT Security Baseline (www.isaca.org)
- ITIL (www.itil.co.uk)
- ISO (www.iso.org)
- ISO 17799 Related Information (www.iso-17799.com/)
- COBIT Case Studies (available at www.itgi.org/ and www.isaca.org)
Questions / Thank You!

Lance M. Turcato, CISA, CISM, CPA
Deputy City Auditor – Information Technology
City of Phoenix
Email: lance.turcato@phoenix.gov
Phone: 602-262-4714

City of Phoenix