Agenda

- Background
- Relating COSO Framework to COBIT 5
- Relating Enterprise Goals & Enablers to Strategy, Governance & Management
- The Continuous Controls Matrix
- The Umbrella IT Governance Framework
- Questions/Dialog
Background - Internal Control Frameworks

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) identifies five components of internal control that need to be in place to achieve financial reporting objectives:
  - Control environment, risk assessment, control activities, information and communications, and monitoring
- The passing of the Sarbanes-Oxley Act (SOX) in 2002 required the accuracy of the financial reporting (Section 302) and resulted in an increased focus on IT controls to support financial reporting processing and assessment (Section 404)
  - Cybersecurity risks have further increased this focus on IT controls
- The COBIT framework (Control Objectives for Information Technology) continues to grow in use to assist with SOX compliance, and is considerably wider in scope with IT general and application controls
COBIT 5 as an IT Governance Framework

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their IT objectives with five overall principles:

- Meeting stakeholder needs
- Covering the enterprise end-to-end
- Applying a single integrated framework
- Enabling a holistic approach
- Separating governance from management

- Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, setting direction and monitoring performance (EDM)
- Management plans, builds, runs and monitors activities in alignment with the direction set by governance to achieve the enterprise objectives (PBRM)
# Relating COSO to COBIT 5

<table>
<thead>
<tr>
<th>COSO Framework Concept</th>
<th>Relevant COBIT 5 Framework Components &amp; Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives</td>
<td>Known as enterprise goals, IT-related goals and enabler goals in COBIT 5</td>
</tr>
<tr>
<td>Process(es)</td>
<td>One enabler type goal is Processes. In COBIT 5, 37 IT-related business processes provide a generic approach to an enterprise’s governance of enterprise IT (GEIT) processes.</td>
</tr>
<tr>
<td>People</td>
<td>The Organizational Structures enabler focuses on how people and their accountabilities and responsibilities are organized to support achievement of the enterprise goals, which include effective internal control arrangements.</td>
</tr>
<tr>
<td>Reasonable assurance</td>
<td>The management process domain Monitor, Evaluate and Assess (MEA) focuses attention on performance and conformance, adequacy of internal control, and external legal and regulatory compliance.</td>
</tr>
<tr>
<td>Adaptable</td>
<td>The COBIT 5 framework aligns with, and is supported by, other more detailed IT-related standards, frameworks and practices with which it aligns.</td>
</tr>
</tbody>
</table>
COBIT 5 Enterprise Goals Cascade (Objectives)
COBIT 5 Enterprise Enablers

1. Principles, Policies and Frameworks
2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies

Resources
COBIT 5 Enterprise IT Domains & Processes

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor
- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise
- AP001 Manage the IT Management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Portfolio
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security

Build, Acquire and Implement
- BA001 Manage Programmes and Projects
- BA002 Manage Requirements Definition
- BA003 Manage Solutions Identification and Build
- BA004 Manage Availability and Capacity
- BA005 Manage Organisational Change Enablers
- BA006 Manage Changes
- BA007 Manage Change Acceptance and Transitioning
- BA008 Manage Knowledge
- BA009 Manage Assets
- BA010 Manage Configuration

Deliver, Service and Support
- DS001 Manage Operations
- DS002 Manage Service Requests and Incidents
- DS003 Manage Problems
- DS004 Manage Continuity
- DS005 Manage Security Services
- DS006 Manage Business Process Controls

Processes for Management of Enterprise IT

Monitor, Evaluate and Assess
- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the Systems of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Continuous Controls Matrix (Reasonable Assurance)

- Key areas to minimize risks during the transition and establish the proper control framework moving forward
  - Functional/Control Areas
    - NIST attributes & COBIT processes
  - Policy / Document Reference
    - Company policies, standards, procedures, and other documents
  - COBIT 5 Identification -
    - Joint effort with Internal Audit
  - SOX cross-reference
    - SOX category and identification
  - Other
    - Other documents & initiatives
Diagram excerpt from COBIT 5 Essential Facts - Fact 4:
“COBIT 5 brings order to complex standards, regulations and frameworks”
Questions

◆ IT is complicated, IT governance doesn’t have to be … visit www.isaca.org/COBIT to begin implementing COBIT5 in your company