COBIT 5 – What’s New, What Auditors Need to Know
June 13th, 2012

Anthony Noble – Viacom Inc.

ISACA COBIT 5 for Assurance
Task Force Chair

Special thanks to Derek Oliver & ISACA for supplying material for this presentation.
Migrating to COBIT 5

- Intro to COBIT 5 for Assurance Professionals
- Types of Assurance
- Audit Methodologies
- COBIT 5 for Assurance Examples
INTRO TO COBIT 5 FOR ASSURANCE PROFESSIONALS
COBIT 5 Initiative

- The COBIT 5 Task Force was created in 2009:
  - Included international experts from across ISACA constituency groups (Assurance, Security Management and Risk/Governance)
  - Co-chair John Lainhart (Past International President)
  - Co-Chair Derek Oliver (Past Chairman of the BMIS Development Committee)

**COBIT 5 Task Force (2009-2011)**
- John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Consulting Services, USA, Co-chair
- Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, MInstISP+, Ravenswood Consultants Ltd, UK, Co-chair
- Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia
- Elisabeth Antonsson, CISM, BSc, BA, Nordea Bank, Sweden
- Steven A. Babb, CGEIT, KPMG, UK
- Steven De Haes, Ph.D., Antwerp Management School, Belgium
- Peter Harrison, CGEIT, FCPA, IBM Australia Ltd., Australia
- Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
- Rob Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, USA
- Erik Pols, CISA, CISM, Shell International-ITCI, Netherlands
- Vernon Poole, CISM, CGEIT, Sapphire, UK
- Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India
The Need?

• More emphasis on operational risk management
  – Need to drive risk management disciplines directly into the day-to-day responsibilities of professionals

• Regulatory bodies requiring more privacy, security and an enhanced control environment
  – Responding to financial crisis
  – Increased publicity and liability

• Workforces are increasingly globalized and distributed, which increases complexities to govern and manage
  – Massive volumes of information – supported by technology – drive business success but also raise a host of complex challenges for business and IT leaders
What is COBIT 5?

A Practical View
Builds on COBIT 4 as a Foundation

- COBIT 5 is a significant strategic evolution of COBIT 4.1

- COBIT 5 is a comprehensive governance and management framework comprising industry practices, analytical tools and models that help an enterprise achieve optimal value and objective by balancing technology:
  - Benefits
  - Risk
  - Resource Use
Shifts from a Technology to a Business Conversation

• Focus on stakeholder objectives:
  – Obtain quality information to support business decisions
  – Generate business value from IT-enabled investments, i.e. achieve strategic goals and realise business benefits through effective and innovative use of IT
  – Achieve operational excellence through reliable and efficient application of technology
  – Maintain IT-related risk at an acceptable level
  – Optimise the cost of IT services and technology
  – Comply with ever-increasing relevant laws, regulations, contractual agreements and policies
COBIT 5 is Generic

- The Framework can be applied to any Enterprise or business process although it does reference Enterprise IT
  - The processes included are needed in any business process not just Enterprise IT
  - Management processes and the monitoring of them is the focus for assurance
  - Area does not need to be using COBIT 5 in order to apply the framework for assurance purposes
Key Concept for Auditors

- COBIT 5 is significant for auditors as it no longer contains any specific Control Objectives except:
  - Enterprise goals should be achieved

- IT Assurance Guide: Using COBIT 4.1 included Control Objectives but the base COBIT 4 did not so is an ongoing trend
What’s in COBIT 5 for Auditors?

Highlights – A Taste!
The initial publication introduces, defines and describes the components that make up the COBIT Framework:

- Principles
- Architecture
- Enablers
- Introduction to implementation guidance and the COBIT process assessment approach
COBIT 5 Principles: Links IT and the Business

- Balance benefits, risk, resources
- Integrates governance of enterprise IT into enterprise governance
- Serve as the overarching framework for governance and management of enterprise IT
- Makes a clear distinction between governance and management
- Defines a set of enablers to support the implementation of a comprehensive governance and management system
Shifts IT Processes to a Business View

- Integrates governance of enterprise IT into enterprise governance
- Covers all functions and processes within the enterprise; COBIT 5 does not focus only on the “IT function”, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
- Considers all IT-related governance and management enablers to be enterprise-wide and end-to-end, i.e. inclusive of everything and everyone, internal and external that is relevant to governance and management of enterprise information and related IT
All enablers have a set of common dimensions.
- provides a common, simple, and structured way to deal with enablers,
- allows to manage their complex interactions, and

The COBIT 5 framework defines seven categories of enablers:
- Processes
- Frameworks, Principles and policies
- Organisational structures
- People, Skills and competencies
- Culture, ethics and behaviour
- Services, Infrastructure & Applications
- Information
Principle 5: Separating Governance from Management

Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against plans.

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.
Immediate Differences: The four MANAGEMENT domains

- Align, Plan & Organise (APO) replaces PO
  - Define & Manage the Enterprise IT Control Framework
- Build, Acquire & Implement (BAI) replaces AI
  - Manage Knowledge
- Deliver, Service & Support (DSS) replaces DS
  - Manage Suppliers
- Monitor, Evaluate & Assess (MEA) replaces ME
  - Provide Assurance (Key management Domain for Auditors)

More meaningful & more “business related”!
Easier to Navigate: Smaller Integrated Publications
Capability vs. Maturity Model

- The process maturity model of COBIT 4.1 has been replaced with a capability model based on ISO/IEC 15504 to align with and support a separate ISACA initiative, the COBIT Program Assessment Model (PAM).
  - Note the Assessment model is not an Assurance model
- There are a number of benefits in doing so:
  - Focus on process is achieving its intended purpose and delivering its required outcomes as expected.
  - Simplification
  - Improved reliability and **repeatability** of process capability assessment
  - Compliance with a generally accepted (ISO) process assessment standard
## Process Capability Model Comparison

<table>
<thead>
<tr>
<th>COBIT 4.1 Maturity Model Levels</th>
<th>COBIT 5 ISO/IEC 15504 Based Capability Levels</th>
<th>Meaning of the COBIT 5 ISO/IEC 15504 Based Capability Levels</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Optimised</td>
<td>5. Optimised</td>
<td>Continuously improved to meet relevant current and projected enterprise goals.</td>
<td></td>
</tr>
<tr>
<td>4. Managed and Measurable</td>
<td>4. Predictable</td>
<td>Operates within defined limits to achieve its process outcomes.</td>
<td></td>
</tr>
<tr>
<td>3. Defined</td>
<td>3. Established</td>
<td>Implemented using a defined process that is capable of achieving its process outcomes.</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>2. Managed</td>
<td>Implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.</td>
<td></td>
</tr>
<tr>
<td>1. Initial/Adhoc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0. Non-existent</td>
<td>0. Incomplete</td>
<td>Not implemented or little or no evidence of any systematic achievement of the process purpose.</td>
<td></td>
</tr>
</tbody>
</table>

**Context**
- Enterprise view/corporate knowledge
- Instance view/individual knowledge
A Practical View

TYPES OF ASSURANCE
What is Assurance?

A three party relationship involving:
- An assurance professional
- A responsible party (responsible for the subject matter); and
- An intended user (of the assurance professional's report)

A subject matter over which the assurance is to be provided (i.e. data, systems, processes)

Suitable criteria against which the subject matter will be assessed (i.e. standards, benchmarks, legislation etc)

An process which the assurance professional will undertake

A conclusion issued by the assurance professional

Taken from IT Assurance Guide: Using COBIT V4.1
Types of Assurance

- IT Assurance Activities include:
  - Perform a risk assessment
  - Diagnose operational and/or project risk
  - Plan/perform risk based assurance activities
  - Assess/Self-assess process maturity
  - Assess/Self-assess controls
  - Substantiate risk
  - Process capability assessments
A Practical View

ASSURANCE METHODOLOGIES
Standard Audit Methodology

- **Audit Planning**
  - Use business goals as a starter
  - Risk assessment/analysis of not meeting goals

- **Define Scope/Objectives of Audit**
  - Examine drivers for the audit
  - Select control objectives for review

- **Execute Audit**
  - Test the controls and their design
  - Document control weaknesses

- **Report an overall conclusion and recommendations**
Example: Assessment Overview

This figure is reproduced from ISO 15504-2:2003 with the permission of ISO at www.iso.org. Copyright remains with ISO.
Examples

A Practitioners View
Change Management

- AI6 in COBIT 4.1 and BAI06 in COBIT 5
- COBIT 4.1 contained a Maturity Model
- COBIT 5 uses the Capability Model
- Will use Emergency Changes for our example
COBIT 4.1 – CO AI6.3 = BAI06.2

• **AI6.3 Emergency Changes**
  – Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process.

• **BAI06.02 Manage Emergency Changes.**
  – Carefully manage emergency changes to minimize further incidents and make sure the change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorized after the change.
For Assurance we can Perform a...

• **Maturity Assessment**
  – Use the COBIT V4.1 Maturity Model

• **Capability Assessment**
  – Use the COBIT Process Assessment Model V4.1

• **Efficiency and Effectiveness of Controls Assessment**
  – Use the IT Assurance Guide: Using COBIT V4.1
  – Use the ISACA Change Management Audit Program which references COBIT4.1
  – Develop a custom audit program using COBIT 5 Process Reference Guide
• Management of the process 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:
  – Level 3 “Defined” when there is a defined formal change management process in place, including categorization, prioritization, emergency procedures, change authorization and release management, and compliance is emerging. Workarounds take place, and processes are often bypassed. Errors may occur and unauthorized changes occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalized, to support planned rollouts of new applications and technologies.
COBIT 4.1 Capability (PAM) Model – AI6

- **Purpose:** Satisfy the business requirement of managing IT changes in alignment with the business strategy to reduce solution and service delivery defects and rework.

- **Outcomes (Os) Number Description**
  - AI6-O1 - Change standards and associated procedures, including those for emergency changes, are defined and communicated.
  - AI6-O2 - Changes are assessed, prioritized and authorized.
  - AI6-O3 - Change status is tracked and reported.

- **Base Practices (BPs)**
  - AI6-BP1 - Develop and implement a process to consistently record, assess and prioritize change requests. *Supports* AI1-O1
  - AI6-BP2 - Assess impact and prioritize changes based on business needs. *Supports* AI1-O2
  - AI6-BP3 - Assure that any emergency and critical change follows the approved process. *Supports* AI1-O1
  - AI6-BP4 - Authorize changes. *Supports* AI1-O2
  - AI6-BP5 - Manage and disseminate relevant information regarding changes. *Supports* AI1-O3
• **Test of Controls – Emergency Changes**
  
  – Enquire whether and confirm that the overall change management process includes emergency change procedures (e.g., defining, raising, testing, documenting, assessing and authorizing emergency changes).
  
  – Inspect the documentation for a representative sample of emergency changes and, by interviewing key staff members, establish whether emergency changes are implemented as specified in the change management process.
  
  – Confirm through interviews with key staff members that emergency access arrangements are authorized, documented and revoked after the change has been applied.
  
  – Enquire whether and confirm that a post-implementation review of emergency changes is conducted.
• Test Samples – Emergency Changes
  – Inspect a sample of emergency changes and verify that they have been processed in accordance with the change management framework. Verify that procedures have been followed to authorize, document and revoke access after the change has been applied.
  – Inspect a sample of emergency changes and determine if a post-implementation review has been conducted after the changes were applied. Consider implications for further application system maintenance, impact on development and test environments, application software development quality, documentation and manuals, and data integrity.
• 6.4.2 Test objective: To verify the effectiveness of the emergency change control process that ensures the integrity of the production libraries and application data.

  – Select a sample of emergency moves to production.
    • Determine if the program was run from an interim library or the production library.
    • If the production library was used, determine if a one-time password was retrieved.
    • Determine if the one-time password was disabled.
Build Your Own Audit Program

• **Process goal**: All emergency changes are reviewed and authorized after the change. Review historical metrics:
  – Percent of total changes that are emergency fixes
  – Number of emergency changes not authorized after the change

• Examine the output for verification:
  – Documented post-implementation review of emergency changes
• **Test that the Base Practice activities are being performed:**
  
  – Ensure that a documented procedure exists to declare, assess, give preliminary approval, authorize after the change and record an emergency change.

  – Verify that all emergency access arrangements for changes are appropriately authorized, documented and revoked after the change has been applied.

  – Monitor all emergency changes, and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity.

  – Define what constitutes an emergency change.
Reference Texts

- IT Assurance Guide: Using COBIT 4.1
- COBIT 5 Overview
- COBIT 5 Enabling Processes
- ISACA Change Management Audit/Assurance Program
- COBIT Process Assessment Model Using 4.1
Questions?