Migrating to COBIT 5 for Auditors
May 10, 2012

Anthony Noble – Viacom Inc.
Rob Johnson – Bank of America

ISACA COBIT 5 for Assurance
Task Force Members

Special thanks to Derek Oliver & ISACA for supplying material for this presentation.
### Speaker Biography

<table>
<thead>
<tr>
<th>Rob Johnson, CISA, CISM, CGEIT, CRISC</th>
<th>Tony Noble, CISA, is the New York based VP of IT audit for Viacom Inc. He has 30 plus years of IT experience and has been employed by major organizations, such as UPS, Coopers &amp; Lybrand and the former Chase Manhattan Bank during his 20 years as an IT auditor. He is a member of the ISACA Framework Committee and is Chair of the COBIT 5 Assurance Guide Task Force. He was a member of the ISACA Guidance and Practices Committee for two years. This committee publishes all methodologies and assurance guidance for ISACA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>has over 20 years experience in information risk, IT audit and privacy/security management. He is currently the senior vice president for IT audit at Bank of America. In his career he has also held leadership roles as head of IT risk for a Global Insurance Company and VP/CISO for large regional bank. Johnson started his career as an architect and worked at a software company where he launched several international commercial software products. He has served on several ISACA committees including chairing the Education Board, member of the Assurance Committee, COBIT 5 Task Force and currently serves on the COBIT 5 Assurance Task Force.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2012 ISACA. All Rights Reserved
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
COBIT: One Framework for the Governance of Enterprise IT

An business framework from ISACA, at www.isaca.org/cobit

Follow us @ISACANews
#NACACS
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 COBIT 5 Framework

- 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
- Makes a clear distinction between governance and management
- Defines a set of enablers to support the implementation of a comprehensive governance and management system
- Serve as the overarching framework for governance and management of enterprise IT
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.

©2012 ISACA. All Rights Reserved
Follow us @ISACAIndia
#NACACS
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”!
### Alignment is now considered to be the result of all governance and management activities.

### Monitor, Evaluate & Assess (MEA)

#### Figure 11—COBIT 4.1 Control Objectives Mapped to COBIT 5

<table>
<thead>
<tr>
<th>COBIT 4.1 Control Objective</th>
<th>Covered in COBIT 5 by</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS13.4 Sensitive Documents and Output Devices</td>
<td>DS57.6</td>
<td></td>
</tr>
<tr>
<td>DS13.5 Preventive Maintenance for Hardware</td>
<td>DS52.2</td>
<td></td>
</tr>
<tr>
<td>ME1.1 Monitoring Approach</td>
<td>MEA1.1</td>
<td></td>
</tr>
<tr>
<td>ME1.2 Definition and Collection of Monitoring Data</td>
<td>MEA1.2, MEA1.3</td>
<td></td>
</tr>
<tr>
<td>ME1.3 Monitoring Method</td>
<td>MEA1.3</td>
<td></td>
</tr>
<tr>
<td>ME1.4 Performance Assessment</td>
<td>MEA1.4</td>
<td></td>
</tr>
<tr>
<td>ME1.5 Board and Executive Reporting</td>
<td>MEA1.4</td>
<td></td>
</tr>
<tr>
<td>ME1.6 Remedial Actions</td>
<td>MEA1.5</td>
<td></td>
</tr>
<tr>
<td>ME2.1 Monitoring of Internal Control Framework</td>
<td>MEA2.1, MEA2.2</td>
<td></td>
</tr>
<tr>
<td>ME2.2 Supervisory Review</td>
<td>MEA2.1</td>
<td></td>
</tr>
<tr>
<td>ME2.3 Control Exceptions</td>
<td>MEA2.4</td>
<td></td>
</tr>
<tr>
<td>ME2.4 Control Self-assessment</td>
<td>MEA2.3</td>
<td></td>
</tr>
<tr>
<td>ME2.5 Assurance of Internal Control</td>
<td>MEA2.6, MEA2.7, MEA2.8</td>
<td></td>
</tr>
<tr>
<td>ME2.6 Internal Control at Third Parties</td>
<td>MEA2.1</td>
<td></td>
</tr>
<tr>
<td>ME2.7 Remedial Actions</td>
<td>MEA2.4</td>
<td></td>
</tr>
<tr>
<td>ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements</td>
<td>MEA3.1</td>
<td></td>
</tr>
<tr>
<td>ME3.2 Optimisation of Response to External Requirements</td>
<td>MEA3.2</td>
<td></td>
</tr>
<tr>
<td>ME3.3 Evaluation of Compliance With External Requirements</td>
<td>MEA3.3</td>
<td></td>
</tr>
<tr>
<td>ME3.4 Positive Assurance of Compliance</td>
<td>MEA3.4</td>
<td></td>
</tr>
<tr>
<td>ME3.5 Integrated Reporting</td>
<td>MEA3.4</td>
<td></td>
</tr>
<tr>
<td>ME4.1 Establishment of an IT Governance Framework</td>
<td>EDM1</td>
<td></td>
</tr>
<tr>
<td>ME4.2 Strategic Alignment</td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>ME4.3 Value Delivery</td>
<td>EDM2</td>
<td></td>
</tr>
<tr>
<td>ME4.4 Resource Management</td>
<td>EDM4</td>
<td></td>
</tr>
<tr>
<td>ME4.5 Risk Management</td>
<td>EDM3</td>
<td></td>
</tr>
<tr>
<td>ME4.6 Performance Measurement</td>
<td>EDM1.3; EDM2.3; EDM3.3; EDM4.3</td>
<td></td>
</tr>
<tr>
<td>ME4.7 Independent Assurance</td>
<td>EDM2.5, EDM2.6, EDM2.7, EDM2.8</td>
<td></td>
</tr>
</tbody>
</table>
The Lens Concept

The Eye of the Beholder: what are you looking for?

COBIT 5 Framework

COBIT 5 For Audit
COBIT 5 For Security
COBIT 5 For Risk
COBIT 5 For ?
COBIT 5 For ?

Other Standards, Frameworks, Guidelines etc
e.g. ISO, ITIL, National Standards.

©2012 ISACA. All Rights Reserved
Easier to Navigate: Smaller Integrated Publications

COBIT 5 Product Family

COBIT 5 Framework

COBIT 5 Enabler Guides
- COBIT 5: Process Reference Guide
- COBIT 5: Information Reference Guide
- Other Enabler Guidance

COBIT 5 Practice Guides
- COBIT 5: Framework Implementation Guide
- COBIT 5 for Security
- COBIT 5 for Assurance
- COBIT 5 for Risk
- Other Practice Guides

COBIT 5 Online Collaborative Environment
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 Assessment Program (CAP).

- 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>Maturity Model Levels</th>
<th>Process Purpose</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COBIT 4.1</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Maturity Model Levels</strong></td>
<td><strong>COBIT 5 ISO/IEC 15504 Based Capability Levels</strong></td>
<td><strong>Meaning of the COBIT 5 ISO/IEC 15504 Based Capability Levels</strong></td>
</tr>
<tr>
<td>5. Optimised</td>
<td>5. Optimised</td>
<td>Continuously improved to meet relevant current and projected enterprise goals.</td>
</tr>
<tr>
<td>4. Managed and Measurable</td>
<td>4. Predictable</td>
<td>Operates within defined limits to achieve its process outcomes.</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>
</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>
</tr>
<tr>
<td>1. Initial/Adhoc</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>
</tr>
</tbody>
</table>
In ISO/IEC 15504 capability levels are defined by a set of nine process attributes; these attributes cover some ground covered by the current COBIT 4 maturity attributes and/or process controls, but only to a certain extent and in a different way.
Benefits of COBIT 5 for Auditors?

A Practical View
Benefits of the Update

The benefits of the new COBIT 5 Process Capability Model compared to the COBIT 4.1 Maturity Models include:

– Auditor can focus on process that assures achieving its purpose and required outcomes.
– Simplifies what testing content eliminating of duplication, because the COBIT 4.1 Maturity Model assessment requires the use of a number of specific components, including the Generic Maturity Model, Process Maturity Models, Control Objectives and Process Controls to support process assessment.
– Improved reliability and repeatability of process capability assessment activities and evaluations, reducing debates and disagreements between stakeholders on assessment results.
– Compliance with a generally accepted process assessment standard and therefore strong support for process assessment approach in the market.
– Increased usability of process capability assessment results, as the new model establishes a basis for more formal, rigorous assessments to be performed, for both internal and potential external purposes.
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

Assessment Overview

Process Reference Model
- Domain and Scope
- Process Purpose
- Process Outcomes

Process Assessment Model
- Scope
- Indicators
- Mapping
- Translation

Measurement Framework
- Capability Levels
- Process Attributes
- Rating Scale

INITIAL INPUT
- Purpose
- Scope
- Constraints
- Identities
- Approach
- Assessor
- Competence Criteria
- Additional Information

ASSESSMENT PROCESS
- Planning
- Data Collection
- Data Validation
- Process Attribute Rating
- Reporting

Roles and Responsibilities
- Sponsor
- Competent Assessor
- Assessor

OUTPUT
- Date
- Assessment Input
- Identification of Evidence
- Assessment Process Used
- Process Profiles
- Additional Information

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

- A16 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
• **AI6.3 Emergency Changes**
  – Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process.

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

• **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
COBIT 4.1 Maturity Model – AI6

- 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 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.
COBIT 4.1 Capability 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, prioritised and authorised.
  - **AI6-O3** - Change status is tracked and reported.

- **Base Practices (BPs)**
  - **AI6-BP1** - Develop and implement a process to consistently record, assess and prioritise change requests. *Supports* AI1-O1
  - **AI6-BP2** - Assess impact and prioritise 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** - Authorise 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 authorising 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 authorised, 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 authorise, 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 authorised after the change. Review historical metrics:
  - Percent of total changes that are emergency fixes
  - Number of emergency changes not authorised after the change

• Examine the output for verification:
  - Documented post-implementation review of emergency changes
Build Your Own Audit Program

• **Test that the Base Practice activities are being performed:**
  – Ensure that a documented procedure exists to declare, assess, give preliminary approval, authorise after the change and record an emergency change.
  – Verify that all emergency access arrangements for changes are appropriately authorised, 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.
Example: Information Quality

Stakeholders—Can be internal or external to the enterprise.
- Information producers, information custodians and information consumers:
  - Information producer, responsible for creating the information
  - Information custodian, responsible for storing and maintaining the information
  - Information consumer, responsible for using the information

Goals:
The goals of information are divided in three sub-dimensions of quality:

**Intrinsic quality**—The extent to which data values are in conformance with the actual or true values. It includes:
- Accuracy—The extent to which information is correct and reliable
- Objectivity—The extent to which information is unbiased, unprejudiced and impartial
- Believability—The extent to which information is regarded as true and credible
- Reputation—The extent to which information is highly regarded in terms of its source or content

**Contextual and representational quality**—The extent to which information is applicable to the task. It includes:
- Relevancy—The extent to which information is applicable and helpful for the task at hand
- Completeness—The extent to which information is not missing and is of sufficient depth and breadth for the task at hand
- Currency—The extent to which information is sufficiently up to date for the task at hand
- Appropriate amount of information—The extent to which the volume of information is appropriate for the task at hand
- Concise representation—The extent to which information is compactly represented
- Consistent representation—The extent to which information is presented in the same format
- Interpretability—The extent to which information is in appropriate languages, symbols, and units, and the definitions are clear
- Understandability—The extent to which information is easily comprehended
- Ease of manipulation—The extent to which information is easy to manipulate and apply to different tasks

**Security/Accessibility quality**—The extent to which information is available or obtainable. It includes:
- Availability—The extent to which information is available when required, or easily and quickly retrievable
- Restricted Access—The extent to which access to information is restricted appropriately to authorised parties
Questions?
Collaborate – Contribute – Connect

- [www.isaca.org/knowledge-center](http://www.isaca.org/knowledge-center)

- The Knowledge Center is a collection of resources and online communities that connect ISACA members – globally, across industries and by professional focus - under one umbrella. Add or reply to a discussion, post a document or link, connect with other ISACA members, or create a wiki by participating in a community today!