Using COBIT5 as an Audit Tool

Ross E. Wescott MA CISA CIA CCP
Chief IT Auditor
Portland General Electric Company
Using COBIT5 as an Audit Tool

Abstract

• IT assurance professionals have successfully used ISACA’s COBIT products for many years. The IT assurance professional focus of these products made them the right tool to perform the right audits of IT.

• However, the IT management and governance focus of COBIT5 is a noticeable departure from previous versions. With the refocus of COBIT, how can the IT Assurance professional take advantage of the advances and concepts of COBIT5 in the performance of their work?
Using COBIT5 as an Audit Tool
About Portland General Electric

- Electric utility serving the northern Willamette Valley in Oregon
- Began in 1889 supplying power to Portland
- Mix of hydropower (22%), coal (25%), gas combustion (28%), wind (11%) and contract power (14%)
- Population in service area: ~1,700,000
- Service Area: ~4,000 sq. mi.
- Cities served: 52
- Total Assets: $6,101,000,000
- 2013 Net Revenue: $1,810,000,000
- MwH Delivered: 21,250,000
- Residential price per kilowatt-hour – 10.8¢ (National Ave.=12.07¢)
Using COBIT5 as an Audit Tool
About Portland General Electric Internal Audit

- Reformed in 2003, after 5 years w/o internal auditing due to parent company: Enron
- Personnel: 1 Director, 4 Staff, 1 Contractor
- Org Chart: IAS reports administratively to the General Counsel with a dotted line to the Board Audit Committee.
- Performance: full scope audits in financial (3%), compliance (5%), IT (8%), operational (65%), and SOx (14%).
- Management requests, corporate projects, and fraud investigations (5%)
Using COBIT5 as an Audit Tool

Learning Objectives

At the end of this session, you will have a better understanding of

- the history of COBIT
- the guiding principles of COBIT 5
- turning COBIT 5 into an IT Audit assurance tool
Using COBIT5 as an Audit Tool
The Journey

• A case study in frustration turned into revelation and resolve
• To a look at how a tool focused on IT management and governance can be turned around to be used by IT assurance.
Using COBIT5 as an Audit Tool
The Conundrum

Before I begin, there is a bit of a conundrum
Using COBIT5 as an Audit Tool
The Conundrum

- I want to set the foundation for COBIT as thoroughly as possible.

But

- There is so much information on COBIT available, it would take days to do it justice.

So
Using COBIT5 as an Audit Tool
The Conundrum

• I will give you a taste of COBIT to get us started.

• The rest, you will have to do on your own.

• But, we will cover COBIT for the Assurance professional more thoroughly.
Using COBIT5 as an Audit Tool
The History of COBIT

• From the ‘70s, a compilation of guidelines, procedures, best practices, and standards for conducting EDP audits entitled "Control Objectives” updated four times between 1980 and 1992.
• COBIT 3rd Edition (2000), Focus: Management Guidelines added
• COBIT 4.0 (2005) and COBIT 4.1 (2007). Focus: Governance and compliance processes added
• COBIT 5.0 (2012) Focus: Assurance processes removed, Full focus on IT governance and management
Using COBIT5 as an Audit Tool
What Is COBIT?

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

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Changes Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

© Portland General Electric Company 2014
© ISACA 2014 All rights reserved. Used with Permission
Using COBIT5 as an Audit Tool
What Is COBIT?

• Target Audience: IT Management

• With a renewed focus on governance by executives and Board, integration of IT with business strategies is paramount.

• If this happens, objectives will be achieved, IT will produce greater value, and current and future technologies will be more useful.

• To that end, COBIT, provides a powerful framework for IT governance and control.
Using COBIT5 as an Audit Tool
What Is COBIT?

And that can be audited.

- **For Gaining Compliance**: because it outlines the steps a business needs to take to be in accordance with legislative constraints by offering a set of best/good practices that will improve weaknesses in IT control areas.

- **For Assessing Risk**: because the uniform approach to IT/business integration can identify and help to mitigate organizational risk for IT and business as a whole.

- **For Achieving Strategy**: because it relates IT-goals to enterprise goals in a goal cascade that help define priorities improvements.
Using COBIT5 as an Audit Tool

What IS COBIT? - The 5 Principles

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance from Management
Using COBIT5 as an Audit Tool
What IS COBIT? - The 5 Principles

• COBIT 5 is based on five key principles for governance and management of enterprise IT:
  – Principle 1: Meeting Stakeholder Needs
  – Principle 2: Covering the Enterprise End-to-End
  – Principle 4: Enabling a Holistic Approach
  – Principle 5: Separating Governance From Management
Using COBIT5 as an Audit Tool

WHAT IS COBIT? The 7 Enablers

• **Principles, policies and frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.

• **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.

• **Organizational structures** are the key decision-making entities in an enterprise.

• **Culture, ethics and behavior** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
Using COBIT5 as an Audit Tool
WHAT IS COBIT - The 7 Enablers

• **Information** is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.

• **Services, infrastructure and applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

• **People, skills and competencies** are required for successful completion of all activities, and for making correct decisions and taking corrective actions.
Using COBIT5 as an Audit Tool
What Is COBIT – The Products

- Also, COBIT Assessment Guide
Using COBIT5 as an Audit Tool
What COBIT Is Not?

• Unlike COBIT (1996) and COBIT 2nd Edition (1998) where the focus was on assurance and the control objective as a bridge from the 1970’s, COBIT 5 is NOT about control objectives.
• In fact, control objectives were gone.
• Control objectives were turned into best or good management practices.
• The audience for the product is not the assurance professional but management. Thus, the assurance professional is seemingly shut out.
• So what was the assurance professional to do when the COBIT product seemed to turn it back on them?
Using COBIT5 as an Audit Tool
What COBIT Is Not?

CRY?
Using COBIT5 as an Audit Tool
What COBIT Is Not?

Get Angry?
Using COBIT5 as an Audit Tool
What COBIT Is Not?

Give Up?
Using COBIT5 as an Audit Tool
What COBIT Is Not?

Or Figure Out How To Make It Work?
Using COBIT5 as an Audit Tool
What COBIT Is Not?

I Decided to Figured It Out!
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

From COBIT 5 – Enabling Processes documentation
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

- **VAL-IT - Framework for Business Technology Management** - set of guiding principles for governance framework, and supporting publications addressing the governance of IT-enabled business investments

- **RISK-IT - Framework for Management of IT Related Business Risks** - provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

<table>
<thead>
<tr>
<th>COBIT 4.1 Control Objective</th>
<th>Covered in COBIT 5 by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC1 Source Data Preparation and Authorisation</td>
<td>DSS06.02; DSS06.03; BAI03.02; BAI03.03; BAI03.05; BAI03.07</td>
</tr>
<tr>
<td>AC2 Source Data Collection and Entry</td>
<td>DSS06.02</td>
</tr>
<tr>
<td>AC3 Accuracy, Completeness and Authenticity Checks</td>
<td>DSS06.02</td>
</tr>
<tr>
<td>AC4 Processing Integrity and Validity</td>
<td>DSS06.02</td>
</tr>
<tr>
<td>AC5 Output Review, Reconciliation and Error Handling</td>
<td>DSS06.02</td>
</tr>
<tr>
<td>AC6 Transaction Authentication and Integrity</td>
<td>DSS06.02</td>
</tr>
<tr>
<td>P01.1 IT Value Management</td>
<td>EDM02</td>
</tr>
<tr>
<td>P01.2 Business-IT Alignment</td>
<td>APO02.01</td>
</tr>
<tr>
<td>P01.3 Assessment of Current Capability and Performance</td>
<td>APO02.02</td>
</tr>
<tr>
<td>P01.4 IT Strategic Plan</td>
<td>APO02.03-05</td>
</tr>
<tr>
<td>P01.5 IT Tactical Plans</td>
<td>APO02.05</td>
</tr>
<tr>
<td>P01.6 IT Portfolio Management</td>
<td>APO05.05</td>
</tr>
<tr>
<td>P02.1 Enterprise Information Architecture Model</td>
<td>APO03.02</td>
</tr>
<tr>
<td>P02.2 Enterprise Data Dictionary and Data Syntax Rules</td>
<td>APO03.02</td>
</tr>
<tr>
<td>P02.3 Data Classification Scheme</td>
<td>APO03.02</td>
</tr>
<tr>
<td>P02.4 Integrity Management</td>
<td>APO01.06</td>
</tr>
<tr>
<td>P03.1 Technological Direction Planning</td>
<td>APO02.03; APO04.03</td>
</tr>
<tr>
<td>P03.2 Technical Infrastructure Plan</td>
<td>APO02.03-05; APO04.03-05</td>
</tr>
</tbody>
</table>

COBIT 4.1 to COBIT5 Mapping - From COBIT 5 – Enabling Processes

© Portland General Electric Company 2014
© ISACA 2014 All rights reserved. Used with Permission
### Using COBIT5 as an Audit Tool

**Assurance Using COBIT5**

<table>
<thead>
<tr>
<th>Val IT 2.0 Key Management Practice</th>
<th>Covered in COBIT 5 by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>VG1.1 Develop an understanding of the significance of IT and the role of governance.</td>
<td>EDM01.01</td>
</tr>
<tr>
<td>VG1.2 Establish effective reporting lines.</td>
<td>EDM01.01</td>
</tr>
<tr>
<td>VG1.3 Establish a leadership forum.</td>
<td>EDM01.02; APO01.01</td>
</tr>
<tr>
<td>VG1.4 Define value for the enterprise.</td>
<td>EDM02.02</td>
</tr>
<tr>
<td>VG1.5 Ensure alignment and integration of business and IT strategies with key business goals.</td>
<td>APO02.01</td>
</tr>
<tr>
<td>VG2.1 Define the value governance framework.</td>
<td>EDM01.02</td>
</tr>
<tr>
<td>VG2.2 Assess the quality and coverage of current processes.</td>
<td>APO01.07</td>
</tr>
<tr>
<td>VG2.3 Identify and prioritise process requirements.</td>
<td>APO01.07</td>
</tr>
<tr>
<td>VG2.4 Define and document the processes.</td>
<td>APO01.07</td>
</tr>
<tr>
<td>VG2.5 Establish, implement and communicate roles, responsibilities and accountabilities.</td>
<td>APO01.02</td>
</tr>
<tr>
<td>VG2.6 Establish organisational structures.</td>
<td>EDM01.02; APO01.02</td>
</tr>
<tr>
<td>VG3.1 Define portfolio types.</td>
<td>EDM02.02</td>
</tr>
<tr>
<td>VG3.2 Define categories (within portfolios).</td>
<td>EDM02.02</td>
</tr>
<tr>
<td>VG3.3 Develop and communicate evaluation criteria (for each category).</td>
<td>EDM02.02</td>
</tr>
<tr>
<td>VG3.4 Assign weightings to criteria.</td>
<td>EDM02.02</td>
</tr>
<tr>
<td>VG3.5 Define requirements for stage-gates and other reviews (for each category).</td>
<td>EDM02.02</td>
</tr>
<tr>
<td>VG4.1 Review current enterprise budgeting practices.</td>
<td>APO06.03</td>
</tr>
</tbody>
</table>

**VAL IT 2.0 to COBIT 5 - From COBIT 5 – Enabling Processes**

© Portland General Electric Company 2014
© ISACA 2014 All rights reserved. Used with Permission
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

<table>
<thead>
<tr>
<th>Risk IT Key Management Practice</th>
<th>Covered in COBIT 5 by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>RG1.1 Perform enterprise IT risk assessment.</td>
<td>EDM03.01; APO12.02-03</td>
</tr>
<tr>
<td>RG1.2 Propose IT risk tolerance thresholds.</td>
<td>EDM03.01</td>
</tr>
<tr>
<td>RG1.3 Approve IT risk tolerance.</td>
<td>EDM03.01-02</td>
</tr>
<tr>
<td>RG1.4 Align IT risk policy.</td>
<td>EDM03.01-02</td>
</tr>
<tr>
<td>RG1.5 Promote IT risk-aware culture.</td>
<td>EDM03.02</td>
</tr>
<tr>
<td>RG1.6 Encourage effective communication of IT risk.</td>
<td>EDM03.03</td>
</tr>
<tr>
<td>RG2.1 Establish and maintain accountability for IT risk management.</td>
<td>EDM03.02</td>
</tr>
<tr>
<td>RG2.2 Co-ordinate IT risk strategy and business risk strategy.</td>
<td>EDM03.01-02</td>
</tr>
<tr>
<td>RG2.3 Adapt IT risk practices to enterprise risk practices.</td>
<td>EDM03.01-02</td>
</tr>
<tr>
<td>RG2.4 Provide adequate resources for IT risk management.</td>
<td>EDM04.01; APO07.01; APO07.03</td>
</tr>
<tr>
<td>RG2.5 Provide independent assurance over IT risk management.</td>
<td>EDM03.03</td>
</tr>
<tr>
<td>RG3.1 Gain management buy-in for the IT risk analysis approach.</td>
<td>EDM01.01-02; EDM03.02</td>
</tr>
<tr>
<td>RG3.2 Approve IT risk analysis.</td>
<td>EDM03.01</td>
</tr>
<tr>
<td>RG3.3 Embed IT risk considerations in strategic business decision making.</td>
<td>EDM03.01</td>
</tr>
<tr>
<td>RG3.4 Accept IT risk.</td>
<td>EDM03.01</td>
</tr>
<tr>
<td>RG3.5 Prioritise IT risk response activities.</td>
<td>EDM03.02</td>
</tr>
<tr>
<td>RE1.1 Establish and maintain a model for data collection.</td>
<td>APO12.01</td>
</tr>
</tbody>
</table>

From RISK IT to COBIT 5: From COBIT 5 – Enabling Processes

© Portland General Electric Company 2014
© ISACA 2014 All rights reserved. Used with Permission
Using COBIT5 as an Audit Tool

Assurance Using COBIT5

- Using COBIT 5 as the foundation
- Using the related linkages to COBIT 4.1, RISK IT, and VAL IT
- And changing the wording of the COBIT5 Management Objectives to turn them into Audit Objectives...

COBIT5 became instantly usable to me as an assurance professional.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

Let’s look at an example.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

Let’s use EDM01 as the basis for our example

<table>
<thead>
<tr>
<th>Detailed Enablers for Assurance Governance and Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EDM01 Ensure Governance Framework Setting and Maintenance</strong></td>
</tr>
<tr>
<td><strong>Area:</strong> Governance <strong>Domain:</strong> Evaluate, Direct and Monitor</td>
</tr>
<tr>
<td><strong>COBIT 5 Process Description</strong></td>
</tr>
<tr>
<td>Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.</td>
</tr>
<tr>
<td><strong>COBIT 5 Process Purpose Statement</strong></td>
</tr>
<tr>
<td>Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparency, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.</td>
</tr>
<tr>
<td><strong>EDM01 Assurance-specific Process Goals and Metrics</strong></td>
</tr>
<tr>
<td><strong>Assurance-specific Process Goals</strong></td>
</tr>
<tr>
<td>1. The strategic objectives and priorities of the assurance function are aligned with the internal and external environment and stakeholder requirements.</td>
</tr>
<tr>
<td>2. The assurance governance system is embedded in the enterprise.</td>
</tr>
<tr>
<td>3. Assurance activities are embedded in business processes.</td>
</tr>
<tr>
<td>4. Assurance is obtained that the assurance function within the enterprise is operating effectively.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

© Portland General Electric Company 2014
© ISACA 2014 All rights reserved. Used with Permission
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

<table>
<thead>
<tr>
<th>Governance Practice</th>
<th>Assurance-specific Inputs (in Addition to COBIT 5 Inputs)</th>
<th>Assurance-specific Outputs (in Addition to COBIT 5 Outputs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM01.01 Evaluate the governance system.</td>
<td>Outside COBIT 5 for Assurance</td>
<td>Stakeholder requirements with regards to governance of assurance</td>
</tr>
</tbody>
</table>

**Assurance-specific Activities (in Addition to COBIT 5 Activities)**

1. Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence the assurance governance design.
2. Identify relevant stakeholders with regards to governance of assurance (business process owners, management, chief auditor, etc.).
3. Collect stakeholder requirements with regards to assurance priorities and objectives.

<table>
<thead>
<tr>
<th>Governance Practice</th>
<th>Assurance-specific Inputs (in Addition to COBIT 5 Inputs)</th>
<th>Assurance-specific Outputs (in Addition to COBIT 5 Outputs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM01.02 Direct the governance system.</td>
<td>EDM01.01</td>
<td>Stakeholder requirements with regards to governance of assurance</td>
</tr>
</tbody>
</table>

**Assurance-specific Activities (in Addition to COBIT 5 Activities)**

1. Obtain senior management commitment to assurance activities.
2. Mandate an enterprise-wide assurance function.

© Portland General Electric Company 2014
© ISACA 2014 All rights reserved. Used with Permission
Using COBIT5 as an Audit Tool

Assurance Using COBIT5

© Portland General Electric Company 2014
© ISACA 2014 All rights reserved. Used with Permission
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

From this direct guidance, ISACA produced an activities table using the enabling processes (1112 of them):

<table>
<thead>
<tr>
<th>Practice ID</th>
<th>Practice Name</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>1. Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.</td>
</tr>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>2. Determine the significance of IT and its role with respect to the business.</td>
</tr>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT.</td>
</tr>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>4. Align the ethical use and processing of information and its impact on society, natural environment, and internal and external stakeholder interests with the enterprise’s direction, goals and objectives.</td>
</tr>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>5. Determine the implications of the overall enterprise control environment with regard to IT.</td>
</tr>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>6. Articulate principles that will guide the design of governance and decision making of IT.</td>
</tr>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>7. Understand the enterprise’s decision-making culture and determine the optimal decision-making model for IT.</td>
</tr>
<tr>
<td>EDM01.01</td>
<td>Evaluate the governance system.</td>
<td>8. Determine the appropriate levels of authority delegation, including threshold rules, for IT decisions.</td>
</tr>
</tbody>
</table>
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

From this, I developed my assessment programs
(This is NOT in our PowerPoint presentation)
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

• All of this I did in the summer of 2013.
• However, ISACA, in the last couple of months, has come up with a surprise.
• By the end of June 2014, they will have a complete set of process assurance programs available.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

• The programs are aligned with generally accepted auditing standards and practices
• Based on a standard assurance engagement approach
• Divided into three familiar audit approach phases:
  – Phase A: Determining the scope/objectives
  – Phase B: Understanding enablers, setting suitable assessment criteria, and performing the assessment
  – Phase C: Communicating and reporting the results
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

A. Determine Scope of the Assurance Initiative

A-1
Determine the stakeholders of the assurance initiative and their stake.

A-2
Determine the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities.

A-3
Determine the enablers in scope and the instance(s) of the enablers in scope.
  - Processes
  - Principles, Policies and Frameworks
  - Organisational Structures
  - Culture, Ethics and Behaviour
  - Information
  - Services, Infrastructure and Applications
  - People, Skills and Competencies

B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment

B-1
Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.

B-2
Obtain understanding of the processes in scope and set suitable assessment criteria. Assess the processes.

B-3
Obtain understanding of the principles, policies and frameworks in scope. Assess principles, policies and frameworks.

B-4
Obtain understanding of the organisational structures in scope. Assess the organisational structures.

B-5
Obtain understanding of the culture, ethics and behaviour in scope. Assess culture, ethics and behaviour.

B-6
Obtain understanding of the information items in scope. Assess information.

B-7
Obtain understanding of the services, infrastructure and applications in scope. Assess services, infrastructure and applications.

B-8
Obtain understanding of the people, skills and competencies in scope. Assess people, skills and competencies.

C. Communicate the Results of the Assessment

C-1
Document exceptions and gaps.

C-2
Communicate the work performed and findings.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

• The audit programs are fully aligned with COBIT 5:
  
  – They explicitly reference all seven enablers. In other words, they are no longer exclusively process-focused; they also use the different dimensions of the enabler model to cover all aspects contributing to the performance of the enablers.

  – They reference the COBIT 5 goals cascade to ensure that detailed objectives of the assurance engagement can be put into the enterprise and IT context, and concurrently they enable linkage of the assurance objectives to enterprise and IT risk and benefits.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

• The audit programs are comprehensive yet flexible.
  – They are comprehensive because they contain assurance steps covering all enablers in detail
  – Yet they are also flexible because this detailed structure enables clear and well-understood scoping decisions to be made.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

• However, in practice, assurance professionals will have to use their own professional judgment to develop their own customized audit programs based on these assurance programs.

• The reason: the programs are very comprehensive, very academic, and, as stated in the guidance, cannot be used directly as is. They must be tailored.

• It is up to the advanced assurance professional to take the material, customize it to their organizations format, and then execute their own version of COBIT5.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

• Let’s look at a sample using EDM01

Ensure governance framework setting and maintenance.

(Note: This is also outside of PowerPoint)

These can be found on ISACA’s web site at:
http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

- A year ago, I started a 5 month project of taking COBIT 5 and doing exactly what ISACA has told us to do in 2014 but without the template.
- I customized COBIT5 for my assurance practice.
- It is much more simple and straightforward and a pragmatic approach.
- I blended, in many cases, COBIT 4.1, VAL IT, and RISK IT with COBIT5 Management Objectives.
- What I came out with in the end was a fully functional audit program that covered all of the COBIT5 supplemented with CobIT 4.1, RISK IT, and VAL IT; over 1100 audit objectives, nearly 1500 tests; all based on these management objectives.
Using COBIT5 as an Audit Tool
Assurance Using COBIT5

And now you can too!
Using COBIT5 as an Audit Tool
The Finish

If you have any questions, please feel free to call and have a meaningful conversation:

Ross Wescott MA CISA CIA CCP
Chief IT Auditor
Portland General Electric Company
503-464-8598
ross.wescott@pgn.com
Using COBIT5 as an Audit Tool
The Real Finish

"That's all folks!"