What is IT governance, and why you need it.

IIA / ISACAWNY Conference – December 11, 2013

Cobit, COSO, and Governance, Oh My!

Don Redman
CISM, CISA, CRISC
Secretary, Certification Coordinator, Director of Research – ISACA Western NY Chapter
Why Governance is important for Safe S-OX

- Considers
  - Enterprise objectives,
  - Known variables, and
  - Requirements of key stakeholders

- Evaluates stakeholder needs
  - through strategic planning

- Sets direction and strategy
  - through prioritized decision-making

- Protects your vulnerable infrastructure

- Monitors performance and compliance, and progress against agreed-on strategy and objectives

But at the end of the day,
- It’s not as much fun as just getting the job done
- We don’t need no stinkin’ governance!
COSO

*Internal Control Integrated Framework*
Why update what works – The Framework has become the most widely adopted control framework worldwide.


Reflect changes in business & operating environments

Expand operations and reporting objectives

Articulate principles to facilitate effective internal control

Updates Context

Broadens Application

Clarifies Requirements


Source: Internal Control Integrated Framework - [www.coso.org](http://www.coso.org)
Update expected to increase ease of use and broaden application

What is *not* changing...

- Core definition of internal control
- Three categories of objectives and five components of internal control
- Each of the five components of internal control are required for effective internal control
- Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness

What is changing...

- Changes in business and operating environments considered
- Operations and reporting objectives expanded
- Fundamental concepts underlying five components articulated as principles
- Additional approaches and examples relevant to operations, compliance, and non-financial reporting objectives added

Source: Internal Control Integrated Framework - [www.coso.org](http://www.coso.org)
Update considers changes in business and operating environments

<table>
<thead>
<tr>
<th>Environments changes...</th>
<th>...have driven Framework updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expectations for governance oversight</td>
<td></td>
</tr>
<tr>
<td>Globalization of markets and operations</td>
<td></td>
</tr>
<tr>
<td>Changes and greater complexity in business</td>
<td></td>
</tr>
<tr>
<td>Demands and complexities in laws, rules, regulations, and standards</td>
<td></td>
</tr>
<tr>
<td>Expectations for competencies and accountabilities</td>
<td></td>
</tr>
<tr>
<td>Use of, and reliance on, evolving technologies</td>
<td></td>
</tr>
<tr>
<td>Expectations relating to preventing and detecting fraud</td>
<td></td>
</tr>
</tbody>
</table>

Source: Internal Control Integrated Framework - [www.coso.org](http://www.coso.org)
Transition & Impact

- Users are encouraged to transition applications and related documentation to the updated Framework as soon as feasible.
- Updated Framework will supersede original Framework at the end of the transition period (i.e., December 15, 2014).
- During the transition period, external reporting should disclose whether the original or updated version of the Framework was used.
- Impact of adopting the updated Framework will vary by organization:
  - Does your system of internal control need to address changes in business?
  - Does your system of internal control need to be updated to address all principles?
  - Does your organization apply and interpret the original framework in the same manner as COSO?
  - Is your organization considering new opportunities to apply internal control to cover additional objectives?

Source: Internal Control Integrated Framework - www.coso.org
Transition & Impact (continued)

• The principles-based approach provides flexibility in applying the Framework to multiple, overlapping objectives across the entity
  – Easier to see what is covered and what is missing
  – Focus on principles may reduce likelihood of considering something that’s irrelevant

• Understanding the importance of specifying suitable objectives focuses on those risks and controls most important to achieving these objectives.

• Focusing on areas of risk that exceed acceptance levels or need to be managed across the entity may reduce efforts spent mitigating risks in areas of lesser significance.

• Coordinating efforts for identifying and assessing risks across multiple, overlapping objectives may reduce the number of discrete risks assessed and mitigated.

Source: Internal Control Integrated Framework - [www.coso.org](http://www.coso.org)
Transition & Impact (continued)

- Selecting, developing, and deploying controls to effect multiple principles may also reduce the number of discrete, layered-on controls.

- Applying an integrated approach to internal control - encompassing operations, reporting, and compliance – may lessen complexity.

- In assessing severity of internal control deficiencies, use only the relevant classification criteria as set out in the Framework or by regulators, standard-setting bodies, and other relevant third parties, as appropriate.

Source: Internal Control Integrated Framework - www.coso.org
What is your IT Governance Experience Index?

Level 4 – Experienced Subject Matter Expert
- “Just here for the **BEER** CPEs – I should have volunteered to teach this workshop.”

Level 3 – Have done some reading / learning
- “Lost in Information Overload”

Level 2 – Just getting started
- “What is that light in the tunnel, an oncoming train?”

Level 1 – Management says we have to
- “Deer in the headlights”

Level 0 – Voted in the last governance election
- “Everyone stop picking on Affordable Health Care!”
COBIT 5
Executive Summary

“I didn't have time to write a short letter, so I wrote a long one instead.” – Mark Twain
Information!

- Information is a key resource for all enterprises.
- Information is created, used, retained, disclosed and destroyed.
- Technology plays a key role in these actions.
- Technology is becoming pervasive in all aspects of business and personal life.

What benefits do information and technology bring to enterprises?
Enterprise Benefits

Enterprises and their executives strive to:

- Maintain 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.

How can these benefits be realised to create enterprise stakeholder value?
Stakeholder Value

- Delivering enterprise stakeholder value requires good governance and management of information and technology (IT) assets.
- Enterprise boards, executives and management have to embrace IT like any other significant part of the business.
- External legal, regulatory and contractual compliance requirements related to enterprise use of information and technology are increasing, threatening value if breached.
- COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.
The COBIT 5 Framework

• Simply stated, COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.

• COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

• The COBIT 5 principles and enablers are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
COBIT 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

Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.
COBIT 5 Enablers

Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.
Governance and 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 agreed-on direction and objectives (EDM).

- **Management** plans, **builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).
COBIT 5 brings together the **five principles** that allow the enterprise to build an effective **governance** and **management** framework based on a holistic set of **seven enablers** that optimises **information** and **technology** investment and use for the benefit of stakeholders.
COBIT 5
Framework Overview
An business framework from ISACA, at www.isaca.org/cobit
COBIT 5 Framework

COBIT 5:
- The main, overarching COBIT 5 product
- Contains the executive summary and the full description of all of the COBIT 5 framework components:
  - The five COBIT 5 principles
  - The seven COBIT 5 enablers plus
  - An introduction to the implementation guidance provided by ISACA (*COBIT 5 Implementation*)
  - An introduction to the COBIT Assessment Programme (not specific to COBIT 5) and the process capability approach being adopted by ISACA for COBIT
COBIT 5 Product Family

Source: COBIT® 5, figure 11. © 2012 ISACA® All rights reserved.
Five COBIT 5 Principles

The five COBIT 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
1. Meeting Stakeholder Needs

Principle 1. Meeting Stakeholder Needs

- Enterprises exist to **create value** for their stakeholders.

Source: COBIT® 5, figure 3. © 2012 ISACA® All rights reserved.
Principle 1. Meeting Stakeholder Needs:

- Enterprises have many stakeholders, and ‘creating value’ means different—and sometimes conflicting—things to each of them.

- Governance is about negotiating and deciding amongst different stakeholders’ value interests.

- The governance system should consider all stakeholders when making benefit, resource and risk assessment decisions.

- For each decision, the following can and should be asked:
  - Who receives the benefits?
  - Who bears the risk?
  - What resources are required?
1. Meeting Stakeholder Needs (cont.)

Principle 1. Meeting Stakeholder Needs:

- Stakeholder needs have to be transformed into an enterprise’s actionable strategy.
- The COBIT 5 goals cascade translates stakeholder needs into specific, actionable and customised goals within the context of the enterprise, IT-related goals and enabler goals.

Source: COBIT® 5, figure 4. © 2012 ISACA® All rights reserved.
1. Meeting Stakeholder Needs

Principle 1. Meeting Stakeholder Needs:
Benefits of the COBIT 5 goals cascade:

- It allows the definition of priorities for implementation, improvement and assurance of enterprise governance of IT based on (strategic) objectives of the enterprise and the related risk.

- In practice, the goals cascade:
  - Defines relevant and tangible goals and objectives at various levels of responsibility.
  - Filters the knowledge base of COBIT 5, based on enterprise goals to extract relevant guidance for inclusion in specific implementation, improvement or assurance projects.
  - Clearly identifies and communicates how (sometimes very operational) enablers are important to achieve enterprise goals.
2. Covering the Enterprise End-to-end

Principle 2. Covering the Enterprise End-to-end:

- COBIT 5 addresses the governance and management of information and related technology from an enterprisewide, end-to-end perspective.

- This means that COBIT 5:
  - Integrates governance of enterprise IT into enterprise governance, i.e., the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system because COBIT 5 aligns with the latest views on 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.
Principle 2. Covering the Enterprise End-to-end

Key components of a governance system
Principle 3. Applying a Single Integrated Framework:

- COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:
  - Enterprise: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
  - IT-related: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI
  - Etc.

- This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.

- ISACA plans a capability to facilitate COBIT user mapping of practices and activities to third-party references.
4. Enabling a Holistic Approach

Principle 4. Enabling a Holistic Approach

COBIT 5 enablers are:

- Factors that, individually and collectively, influence whether something will work—in the case of COBIT, governance and management over enterprise IT.
- Driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve.
- Described by the COBIT 5 framework in seven categories.
Principle 4. Enabling a Holistic Approach

Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.
4. Enabling a Holistic Approach (cont.)

Principle 4. Enabling a Holistic Approach:

1. **Processes**—Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals

2. **Organisational structures**—Are the key decision-making entities in an organisation

3. **Culture, ethics and behaviour**—Of individuals and of the organisation; very often underestimated as a success factor in governance and management activities

4. **Principles, policies and frameworks**—Are the vehicles to translate the desired behaviour into practical guidance for day-to-day management

5. **Information**—Is pervasive throughout any organisation, i.e., deals with all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.

6. **Services, infrastructure and applications**—Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services

7. **People, skills and competencies**—Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions

Principle 4. Enabling a Holistic Approach:

- Systemic governance and management through interconnected enablers—To achieve the main objectives of the enterprise, it must always consider an interconnected set of enablers, i.e., each enabler:
  - Needs the input of other enablers to be fully effective, e.g., processes need information, organisational structures need skills and behaviour
  - Delivers output to the benefit of other enablers, e.g., processes deliver information, skills and behaviour make processes efficient
- This is a KEY principle emerging from the ISACA development work around the Business Model for Information Security (BMIS).

**Principle 4. Enabling a Holistic Approach**

**COBIT 5 Enabler Dimensions:**

- All enablers have a set of common dimensions. This set of common dimensions:
  - Provides a common, simple and structured way to deal with enablers
  - Allows an entity to manage its complex interactions
  - Facilitates successful outcomes of the enablers

---

### Enabler Dimension

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Goals</th>
<th>Life Cycle</th>
<th>Good Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Internal Stakeholders</td>
<td>- Intrinsic Quality</td>
<td>- Plan</td>
<td>- Practices</td>
</tr>
<tr>
<td>- External Stakeholders</td>
<td>- Contextual Quality (Relevance, Effectiveness)</td>
<td>- Design</td>
<td>- Work Products (Inputs/Outputs)</td>
</tr>
<tr>
<td></td>
<td>- Accessibility and Security</td>
<td>- Build/Acquire/Create/Implement</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Use/Operate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Evaluate/Monitor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Update/Dispose</td>
<td></td>
</tr>
</tbody>
</table>

---

### Enabler Performance Management

- Are Stakeholders Needs Addressed?
- Are Enabler Goals Achieved?
- Is Life Cycle Managed?
- Are Good Practices Applied?

**Metrics**

- Metrics for Achievement of Goals (Lag Indicators)
- Metrics for Application of Practice (Lead Indicators)

---

Source: COBIT® 5, figure 13. © 2012 ISACA® All rights reserved.
5. Separating Governance From Management

Principle 5. Separating Governance From Management:

- The COBIT 5 framework makes a clear distinction between governance and management.
- These two disciplines:
  - Encompass different types of activities
  - Require different organisational structures
  - Serve different purposes
- **Governance**—In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.
- **Management**—In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.
Principle 5. Separating Governance From Management:

- **Governance** ensures that stakeholders needs, conditions and options are **evaluated** to determine balanced, agreed-on enterprise objectives to be achieved; setting **direction** through prioritisation and decision making; and **monitoring** performance and compliance against agreed-on direction and objectives (EDM).

- **Management plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).
Principle 5. Separating Governance From Management:
COBIT 5 is not prescriptive, but it advocates that organisations implement governance and management processes such that the key areas are covered, as shown.
5. Separating Governance From Management (cont.)

Principle 5. Separating Governance from Management:

- The COBIT 5 framework describes seven categories of enablers (*Principle 4*). Processes are one category.

- An enterprise can organise its processes as it sees fit, as long as all necessary governance and management objectives are covered. Smaller enterprises may have fewer processes; larger and more complex enterprises may have many processes, all to cover the same objectives.

- COBIT 5 includes a **process reference model (PRM)**, which defines and describes in detail a number of governance and management processes. The details of this specific enabler model can be found in the *COBIT 5: Enabling Processes* volume.
COBIT 5: Enabling Processes
**COBIT 5: Enabling Processes**

- *COBIT 5: Enabling Processes* complements *COBIT 5* and contains a detailed reference guide to the processes that are defined in the COBIT 5 process reference model:
  - In Chapter 2, the COBIT 5 goals cascade is recapitulated and complemented with a set of example metrics for the enterprise goals and the IT-related goals.
  - In Chapter 3, the COBIT 5 process model is explained and its components defined.
  - Chapter 4 shows the diagram of this process reference model.
  - Chapter 5 contains the detailed process information for all 37 COBIT 5 processes in the process reference model.
COBIT 5: Enabling Processes (cont.)
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 Enablement
- 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

Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.
COBIT 5: Enabling Processes

The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management—with management further divided into domains of processes:

- The GOVERNANCE domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
- The four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor (PBRM).
COBIT 5 Implementation
COBIT 5 Implementation

• The improvement of the governance of enterprise IT (GEIT) is widely recognised by top management as an essential part of enterprise governance.

• Information and the pervasiveness of information technology are increasingly part of every aspect of business and public life.

• The need to drive more value from IT investments and manage an increasing array of IT-related risk has never been greater.

• Increasing regulation and legislation over business use of information is also driving heightened awareness of the importance of a well-governed and managed IT environment.
ISACA has developed the COBIT 5 framework to help enterprises implement sound governance enablers. Indeed, implementing good GEIT is almost impossible without engaging an effective governance framework. Best practices and standards are also available to underpin COBIT 5.

Frameworks, best practices and standards are useful only if they are adopted and adapted effectively. There are challenges that need to be overcome and issues that need to be addressed if GEIT is to be implemented successfully.

**COBIT 5: Implementation** provides guidance on how to do this.
COBIT 5 Implementation (cont.)

- **COBIT 5: Implementation** covers the following subjects:
  - Positioning GEIT within an enterprise
  - Taking the first steps towards improving GEIT
  - Implementation challenges and success factors
  - Enabling GEIT-related organisational and behavioural change
  - Implementing continual improvement that includes change enablement and programme management
  - Using COBIT 5 and its components
COBIT 5 Implementation (cont.)

Source: COBIT® 5, figure 17. © 2012 ISACA® All rights reserved.
COBIT 5
Future Supporting Products
COBIT 5 Product Family

Source: COBIT® 5, figure 11. © 2012 ISACA® All rights reserved.
COBIT 5 Future Supporting Products

Future supporting products:

- **Professional Guides:**
  - COBIT 5 for Information Security
  - COBIT 5 for Assurance
  - COBIT 5 for Risk
- **Enabler Guides:**
  - COBIT 5: Enabling Information
- **COBIT Online Replacement**
- **COBIT Assessment Programme:**
  - Process Assessment Model (PAM): Using COBIT 5
  - Assessor Guide: Using COBIT 5
  - Self-assessment Guide: Using COBIT 5
COSO vs COBIT – Your Thoughts?

**COSO ERM Framework**
- Enterprise Risk Management
  - Financial
  - Operational
  - Compliance
  - Strategic

**COBIT 5**
- IT Governance and Management
  - Plan
  - Build
  - Run
  - Monitor
Cobit 5 Product Family

- Cobit 5 Framework
  - COBIT 5 is the overarching business and management framework for governance and management of enterprise IT. This volume documents the 5 principles of COBIT 5 and defines the 7 supporting enablers.

- Translations Available

<table>
<thead>
<tr>
<th>Languages available now – more coming!</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanish</td>
</tr>
<tr>
<td>Romanian</td>
</tr>
</tbody>
</table>
Cobit 5 Enabler Guides

- Cobit 5 Enabling Processes
  - Includes the COBIT 5 goals cascade, a process model explanation and the process reference model.

- Cobit 5 Enabling Information
  - This guide further explains the Information Model (based on the COBIT 5 generic enabler model) and provides examples of fully elaborated information entities.
Cobit 5 Professional Guides

- **Cobit 5 Implementation**
  - Provides a good practice approach for implementing GEIT based on a continual improvement life cycle that should be tailored to suit the enterprise’s specific needs.
  - Cobit 5 Toolkit Supplement – Resources include presentations for multiple org layers, examples, case studies and FAQs (inc. Management Awareness Diagnostic Scorecard).

- **Cobit 5 for Information Security— $35 ($175 non-member)**
  - Information security is essential in the day-to-day operations of enterprises, which must ensure confidentiality and integrity of their information, while providing availability to those who have business reasons to use it.
Cobit 5 Professional Guides (cont.)

- **Cobit 5 for Assurance**
  - Focuses on assurance and provides more detailed and practical guidance for assurance professionals and other interested parties at all levels of the enterprise on how to use COBIT 5 to support a variety of IT assurance activities.

- **Cobit 5 for Risk**
  - Serves as the information risk specific guidance as it relates to COBIT for ISACA’s information risk constituents. The guide should be considered the risk focused equivalent of the COBIT 5 for Information Security publication within the COBIT 5 family of products.
Cobit 5 Professional Guides (cont.)

- Cobit 5 Assessment Program
  - The basis for assessing an enterprise’s processes to determine process capability for the governance and management of IT and related services.
  - Process Assessment Model
    - The PAM combines COBIT 5 with ISO/IEC 15504-2, and provides the basis for a robust, dependable assessment approach.
  - Assessor Guide
    - This PAM companion details how to undertake an assessment based on ISO/IEC 15504-2.
  - Self-Assessment Guide
    - This PAM companion provides an alternative and less rigorous approach to performing an assessment.
Backup
What is the purpose of COBIT 5?

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information and technology assets (IT).

Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
Where are the control objectives in COBIT 5?

Based on five principles and seven enablers, COBIT 5 uses governance and management practices to describe actions that are examples of good practices to effect governance and management over enterprise IT. Many of these practices and the supporting activities exert ‘control’ over the process to deliver the required outcome.

The move from the control objectives term was explained in an ISACA Journal article, Volume 4, 2011, written by one of COBIT’s first contributors, Erik Guldentops.
Can I use COBIT 5 as a statement of criteria for specific audit conclusions?

There are additional professional guides that extend COBIT 5. Amongst these is COBIT 5 for Assurance.

This serves as the guide for assurance professionals wanting to use COBIT 5 in their work. COBIT 5 for Assurance provides comprehensive guidance on using COBIT 5 to support assurance activities.
In what way can I suggest to executive management that it use COBIT 5?

Because COBIT is business-oriented, using it to deliver value and govern and manage IT-related business risk is straightforward. The COBIT 5 two-page executive summary and supporting short presentation can be used in the discussion with management. The goals cascade in the framework can be used to:

- Determine stakeholder needs and governance objectives (value creation)
- Identify enterprise goals that can support stakeholder needs. If the balanced scorecard (BSC) is used to develop these goals, then a common set of terms can be used to communicate the goals. Enterprise goals from the BSC are reproduced in figure 5 on page 19 of COBIT 5.
- Select IT-related goals (for each enterprise goal) that will facilitate the achievement of the goals. IT-related goals can be found in figure 6 on page 19 of COBIT 5.
- Achieve IT-related goals. This requires the successful application and use of enablers. The framework describes enablers in detail in chapter 5. One of the enablers, processes, is treated separately in the COBIT 5: Enabling Processes publication.
- Present the proposed set of needs, goals and enablers to executive management as a means of delivering effective governance and management of IT-related technology.
What is the quickest and best way to convince key executives and other enterprise stakeholders of the value of using COBIT 5?

The enterprise’s culture is vitally important. A proactive culture will be more receptive than one that is not proactive; however, consider emphasizing COBIT’s focus on stakeholder value creation, it being business driven, its alignment with other internationally recognized standards and frameworks, and its simple, but complete, structure. COBIT 5 is based on five principles and seven enablers. All other governance and management guidance in COBIT 5 cascade from these basic areas.
Sources – For more information

- ISACA – www.ISACA.org
  - Search “COBIT”

Don.Redman@Xerox.com
CLOUD
I REMEMBER A TIME WHEN I HAD TO LISTEN TO THE TOPIC AT HAND BEFORE ADDING MY INSINCERE INPUT.

I THINK WE SHOULD VIRTUALIZE THE PROCESS AND MOVE IT TO THE CLOUD.

HEY, THAT'S A GREAT IDEA!

NOW IT'S JUST ALL TOO EASY.

I HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO CLOUD COMPUTING.

BLAH BLAH CLOUD. BLAH BLAH CLOUD. BLAH BLAH CLOUD. BLAH BLAH CLOUD.

IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!

/// BLAH BLAH PLATFORM.
Cloud Computing – It’s Ubiquitous!

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction....” (NIST SP800-145)

“...As browsers that are capable of efficiently displaying interactive content have become ubiquitous, SaaS application deployment has become increasingly convenient and efficient with little or no client-side software required.... As the ubiquity and performance of the Internet have increased, SaaS has become nearly universally applicable.” (NIST SP800-146)

“Because of their ubiquity, Web browsers are a key element for client-side access to cloud computing services.” (NIST 800-144)

“The promise of cloud computing is arguably revolutionizing the IT services world by transforming computing into a ubiquitous utility....” (ISACA Cloud Computing Resarch Oct. 2009)
...ahem, what’s “Ubiquitous”? 

- Ubiquitous
  - Adjective: existing or being everywhere at the same time: constantly encountered: widespread <a ubiquitous fashion>
C.L.O.U.D.® Computing

“Acronymizing” The Cloud

ACRONYM: A Cryptic Reminder Of Names You Meet

- Cyber
- Layered
- Outsourced
- Ubiquitous
- Data

C3 - C.L.O.U.D. Computing Compliance
New Intermediation Layer: Cloud Service Brokers

It's Ubiquitous!
Selling the Cloud: Cloud Service Brokers

- **Liaison:**
  - Creates and maintains relationships with service providers.
  - Select best provider and/or service for customer
  - Monitoring /reporting services
  - Typically has no cloud resources of its own.

- **Managed Services Provider:**
  - Manages use of services
  - Oversees performance and Service Level Metrics
  - Negotiates Relationships between customers and providers.
  - Typically has no cloud resources of its own.

*Source: IT Law Wiki*
Cloudy Issues: Multi - Tenancy

One cloud may be serving multiple customers - would **YOU** rent a locker here?

ISACA Webinar, July 2011: Cloud Security Delivery Models: Risks & Recommendations
Cloudy Issues: Anyone can move in next door!

You can’t pick your neighbor” in a cloud service. Anyone in the world with access to a credit card number can purchase cloud services and be running in minutes.
Cloudy Issues: Neighbors (or Vendors) Drawing Attention

What if the neighbor or vendor has a vested interest in promoting their cloud location?

ISACA Webinar, July 2011: Cloud Security Delivery Models: Risks & Recommendations
Cloudy Issues: Layered Outsourcing

- The cloud provider may leverage other vendors for their business delivery model.
  - Example: SaaS provider outsources to a PaaS provider.
  - Map your data flow and control ownership from Input to Output, and User to Storage to Bare Metal.
Challenge – CIA “Triad”

- The cloud provider business/profit model depends on architectural and operational efficiencies that make it difficult to identify, document, and establish control frameworks – and ownership.
  - Confidentiality
  - Integrity
  - Availability
- Follow the data!
Your neighbors and You – What elements are shared?
Change & Configuration Management, Privileged Access...
Lessons Learned

- recognize mistakes
- observe what works
- document them
- share them
Auditing the Cloud – Lessons Learned

- Customer Relationship Management and Sales process hosted at two integrated SaaS providers, internal IT managed the API.
- SAS 70 detailed SaaS vendor outsourced IaaS to 2 data centers
- Further inquiry revealed relocated data center and SaaS provider actually outsourced PaaS.
- Inspection of Master Service Agreement indicated that customer was paying for a “Dedicated Pod” with dedicated web server / db (with end-of-life technology)
  - RH Linux 5 / Oracle 10.x DB
  - Inquired with vendor to validate, 3-week turnaround to confirm platform had been updated to Oracle 11g. Business continued in the middle of pilot, did not intervene or support escalation, even under threat of cancelling launch.
- What is a “dedicated pod”? 

5 June 2012
Summary

- Effective auditing of cloud controls requires a multi-disciplinary, cross-organizational analysis. You must be proactive in documenting your multi-dimensional control grid, and understanding the implied RASCI* matrix.
- P6 – Proper Prior Planning Prevents Poor Performance!
  - Effective preparation begins with the outsourcing effort!
- Leverage available control frameworks and tools to ensure you have not forgotten something.
- Think “Layered Outsourcing” and “Supply Chain Management”

* RACI / RASCI – Responsible, Accountable, Supports, Communicate, Inform
Summary (cont.)

- Evaporate the hype and confusion surrounding Cloud Computing by changing the conversation.
- Talk about layered outsourcing
- Make analogies to supply chain management
- Document controls thoroughly with attention to
  - Roles & Responsibilities
  - Boundaries
  - Handoffs
  - Communication Protocols
Summary (cont.)

- Work with a vendor who will “bake security in”
- Document compliance and security control requirements, and provide to vendor as part of business requirements.
  - Xerox awarded State of Texas contract for Govt. Services Cloud.
- Don’t forget contracts, SLAs, metrics.
Sources – For more information

- ISACA – [www.ISACA.org](http://www.ISACA.org)
- Cloud Security Alliance – [www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)
- European Network and Information Security Agency (enisa) - [www.enisa.europa.eu](http://www.enisa.europa.eu)
- National Institute of Standards and Technology - [www.nist.gov](http://www.nist.gov)

Don.Redman@Gmail.com