RELATING THE COSO INTERNAL CONTROL—INTEGRATED FRAMEWORK AND COBIT

AN ISACA COBIT SERIES WHITE PAPER

This white paper takes the refreshed and updated COSO Internal Control—Integrated Framework (the COSO framework) as its base structure and examines how the relevant components and content of the COBIT 5 framework and its supporting guidance deliverables relate to the COSO framework. Through the efforts of many (including ISACA), the refreshed COSO framework places much stronger emphasis on the importance of information technology, in addition to other enhancements within its principles.

The purpose of this white paper is to highlight areas of alignment and differences in the content of the frameworks, and also to help enterprises that are using the COSO framework by presenting the relationship between the COSO framework guidance and the COBIT 5 framework guidance.

ISACA®
Trust in, and value from, information systems

COBIT® 5
AN ISACA® FRAMEWORK

Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: www.isaca.org

Provide feedback:
www.isaca.org/COSO-and-COBIT

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
ISACA (Official),
http://linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ISACA®

With more than 110,000 constituents in 180 countries, ISACA *(www.isaca.org)* helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, the nonprofit, independent ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. These professionals rely on ISACA as the trusted source for information and technology knowledge, community, standards and certification. The association, which has 200 chapters worldwide, advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. ISACA also developed and continually updates COBIT®, a business framework that helps enterprises in all industries and geographies govern and manage their information and technology.

DISCLAIMER

ISACA has designed and created *Relating the COSO Internal Control—Integrated Framework and COBIT* (the "Work") primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights© 2014 ISACA. All rights reserved. For usage guidelines, see *www.isaca.org/COBITuse*

ACKNOWLEDGMENTS

Expert Reviewers

Steven A. Babb
CGEIT, CRISC, ITIL, Vodafone, UK

Frank J. Cindrich
CGEIT, CIPP, CIPP/G, Deloitte & Touche LLP, USA

Joanne De Vito De Palma
BCMM, The Ardent Group, USA

Jimmy Heschl
CISA, CISM, CGEIT, ITIL Expert,
bwin.party digital entertainment plc, Austria

Katherine McIntosh
CISA, Central Hudson Gas & Electric Corp., USA

Mario C. Micallef
CGEIT, CPAA, FIA, Malta

Anthony P. Noble
CISA, Viacom, USA

Andre Pitkowski
CGEIT, CRISC, APIT Informatica, Brazil

Kenneth L. Vander Wal
CISA, CPA, Ernst & Young LLP (retired), USA

Ross E. Wescott
CISA, Portland General Electric, USA

ISACA Board of Directors

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA,
Queensland Government, Australia, International President

Allan Boardman
CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP,
Morgan Stanley, UK, Vice President

Juan Luis Carselle
CISA, CGEIT, CRISC, RadioShack, Mexico, Vice President

Ramses Gallego
CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt,
Dell, Spain, Vice President

Theresa Grafenstine
CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA,
US House of Representatives, USA, Vice President

Vittal Raj
CISA, CISM, CGEIT, CFE. CIA, CISSP, FCA, Kumar & Raj,
India, Vice President

Jeff Spivey
CRISC, CPP, PSP, Security Risk Management Inc., USA,
Vice President

Marc Vael, Ph.D.
CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium,
Vice President

Gregory T. Grocholski
CISA, The Dow Chemical Co., USA,
Past International President

Kenneth L. Vander Wal
CISA, CPA, Ernst & Young LLP (retired), USA,
Past International President

Christos K. Dimitriadis, Ph.D.
CISA, CISM, CRISC, INTRALOT S.A., Greece, Director

Krysten McCabe
CISA, The Home Depot, USA, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich,
Australia, Director

Knowledge Board

Christos K. Dimitriadis, Ph.D.
CISA, CISM, CRISC, INTRALOT S.A., Greece, Chairman

Rosemary M. Amato
CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd.,
The Netherlands

Steven A. Babb
CGEIT, CRISC, Vodafone, UK

Thomas E. Borton
CISA, CISM, CRISC, CISSP, Cost Plus, USA

Phil J. Lageschulte
CGEIT, CPA, KPMG LLP, USA

Anthony P. Noble
CISA, Viacom, USA

Jamie Pasfield
CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK

Framework Committee

Steven A. Babb
CGEIT, CRISC, Vodafone, UK, Chairman

David Cau
GRCP, ITIL V3, MSP, Deloitte, Luxembourg

Sushil Chatterji
CGEIT, Edutech Enterprises, Singapore

Frank J. Cindrich
CGEIT, CIPP, CIPP/G, Deloitte & Touche LLP, USA

Joanne De Vito De Palma
BCMM, The Ardent Group, USA

Jimmy Heschl
CISA, CISM, CGEIT, ITIL Expert,
bwin.party digital entertainment plc, Austria

Katherine McIntosh
CISA, Central Hudson Gas & Electric Corp., USA

Andre Pitkowski
CGEIT, CRISC, APIT Informatica, Brazil

Paras Kesharichand Shah
CISA, CGEIT, CRISC, CA, Vital Interacts, Australia

Reservation of Rights© 2014 ISACA. All rights reserved.

BACKGROUND

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework and the ISACA COBIT framework have a long and beneficial history of in-tandem use by many enterprises, long before the Sarbanes-Oxley Act of 2002 regulations were enacted. With the advent of this set of regulatory challenges, enterprises were compelled to use COSO for their financial framework (the US Securities and Exchange Commission [SEC] mentioned the COSO framework[1] as one of the sources of guidance for evaluating internal control over financial reporting). These same enterprises were also drawn to COBIT for their IT control framework guidance, because of the specific *IT Control Objectives for Sarbanes Oxley* product that ISACA published and their recognition of IT as a critical enabler to the operation of strong financial controls. In May 2013, COSO released its updated and refreshed Internal Control—Integrated Framework. ISACA participated in this update program, serving as a member of the COSO Advisory Council. Meanwhile, ISACA released COBIT 5[2], its update and revision to COBIT, in April 2012. Because many enterprises rely on the use of both frameworks internally and many others use both frameworks in their consulting work, ISACA realized the natural need to consider how the two frameworks relate to each other. For this reason, ISACA developed this white paper to present the ISACA perspective on the relationship between the two frameworks and to support dialogue among professionals who use the frameworks.

PURPOSE

This white paper takes the refreshed and updated COSO Internal Control—Integrated Framework (the COSO framework) as its base structure and examines how the relevant components and content of the COBIT 5 framework and its supporting guidance deliverables relate to the COSO framework. Through the efforts of many (including ISACA), the May 2013 refreshed COSO framework places much stronger emphasis on the importance of information technology, in addition to other enhancements within its principles.

The purpose of this white paper is to highlight areas of alignment and differences in the content of the frameworks, and also to help enterprises that are using the COSO framework by presenting the relationship between the COSO framework guidance and the COBIT 5 framework guidance.

Note: It is assumed that the readers of this white paper have an understanding of the COSO and COBIT 5 framework concepts and components, which are freely available in foundational reference publications, on each organization's web site. Therefore, repeating content from these reference publications is kept to a minimum in this white paper.

SUMMARY CONCLUSION

Many enterprises ask, "With the update of both the COSO Internal Control—Integrated Framework and the COBIT framework, are they still complementary and compatible?" The answer to this question is yes, the frameworks are complementary and compatible as guidance to support the assessment and improvement of internal control practices and activities within the governance and management arrangements of an enterprise.

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Internal Control—Integrated Framework (2013)," USA, 2013, *www.coso.org/IC.htm*

[2] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,* USA, 2012, *www.isaca.org/COBIT*

THE COSO INTERNAL CONTROL—INTEGRATED FRAMEWORK

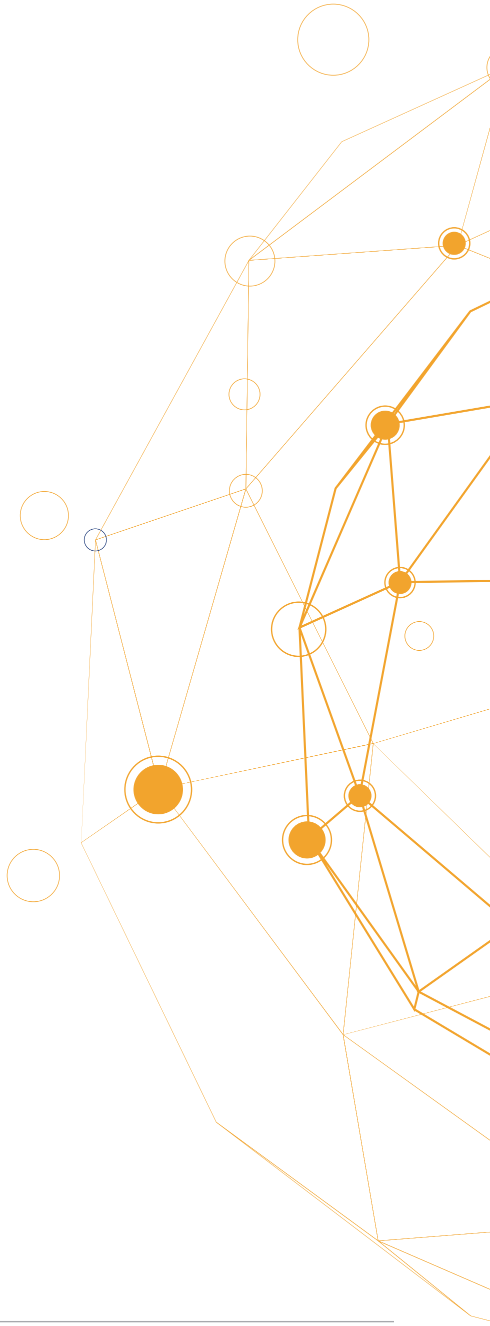
“The *Framework* assists management, boards of directors, external stakeholders, and others interacting with the entity in their respective duties regarding internal control without being overly prescriptive. It does so by providing both understanding of what constitutes a system of internal control and insight into when internal control is being applied effectively.”

“Internal control is defined as follows:

> *Internal control is a process, affected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

“This definition reflects certain fundamental concepts. Internal control is:

- *Geared to the achievement of objectives* in one or more categories—operations, reporting, and compliance
- A *process* consisting of ongoing tasks and activities—a means to an end, not an end in itself
- *Effected by people*—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control
- Able to *provide reasonable assurance*—but not absolute assurance, to an entity’s senior management and board of directors
- *Adaptable to the entity structure*—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process”[3]



[3] COSO, “Internal Control–Integrated Framework Executive Summary,” USA, May 2013, *www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf.* Used with permission.

Reservation of Rights© 2014 ISACA. All rights reserved.

COBIT 5: BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

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

COBIT 5 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, encompassing the full end-to-end business and IT functional areas of responsibility and considering the IT-related interests of internal and external stakeholders. COBIT 5 uses *enablers*, which are broadly defined as anything that can help to achieve the objectives of the enterprise. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*[4] (hereafter referred to as “COBIT 5 framework”) defines seven categories of enablers.

[4] *Op cit ISACA*

Reservation of Rights© 2014 ISACA. All rights reserved.

How COSO Framework Fundamental Concepts Relate to COBIT 5 Framework Components and Content

Figure 1 summarizes the relationship of COBIT 5 framework components with the fundamental concepts of the COSO framework.

FIGURE 1—COSO RELATED TO COBIT 5

COSO Framework Concept	Relevant COBIT 5 Framework Components and Content
Objectives	Known as enterprise goals, IT-related goals and enabler goals in COBIT 5, these goals form the goals cascade (**figure 5**) and identify the focus of the COBIT 5 framework. The enterprise and IT-related goals are generic and based on the four quadrants of the balanced scorecard (BSC) approach.[5] The enabler goals are part of the COBIT 5 generic enabler model and address intrinsic quality, contextual quality, and security and accessibility objectives.
Process(es)	The COBIT 5 framework is built on seven types of governance and management enablers, which are used to varying degrees by all enterprises to achieve their business goals. One enabler type is Processes. In COBIT 5, 37 IT-related business processes provide an illustrative generic approach to an enterprise's governance of enterprise IT (GEIT) processes. The process guidance that supports COBIT 5 includes control practices and their activities. Many COBIT users are process-oriented because processes were the predominant focus in earlier COBIT versions. The *COBIT 5: Enabling Processes* guide details the 37 COBIT 5 processes. Specific consideration of the relationship between the COSO framework principles and the COBIT 5 framework process guidance is a focus of this white paper (see the appendix for a table summary).
People	People are very important in the COBIT 5 framework and are addressed in its People, Skills and Competencies enabler. The Organisational Structures enabler focuses on how people and their accountabilities and responsibilities are organized to support achievement of the enterprise goals, which include effective internal control arrangements. The COBIT 5 Processes enabler guidance for the RACI (responsible, accountable, consulted, informed) charts links people's roles to processes.
Reasonable assurance	COBIT 5 provides a sound basis on which assurance over GEIT arrangements can be provided. In particular, the management process domain Monitor, Evaluate and Assess (MEA) focuses attention on performance and conformance, adequacy of internal control, and external legal and regulatory compliance. At the governance level, the EDM05 *Ensure stakeholder transparency* process ensures that communications with stakeholders is effective and timely. The *COBIT 5 for Assurance* professional guide provides specific guidance for assurance provision based on COBIT 5.
Adaptable	COBIT 5 is a flexible framework that can be adapted to support the design, development and implementation of GEIT arrangements within an enterprise. The COBIT 5 framework aligns with, and is supported by, other more detailed IT-related standards, frameworks and practices with which it aligns. The *COBIT 5 Implementation* guide describes how COBIT 5 guidance can be adapted to support the enterprise.

The COSO and COBIT 5 frameworks are applicable to all enterprises, irrespective of size, location or industry type.

[5] Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard University Press, USA, 1996

Reservation of Rights© 2014 ISACA. All rights reserved.

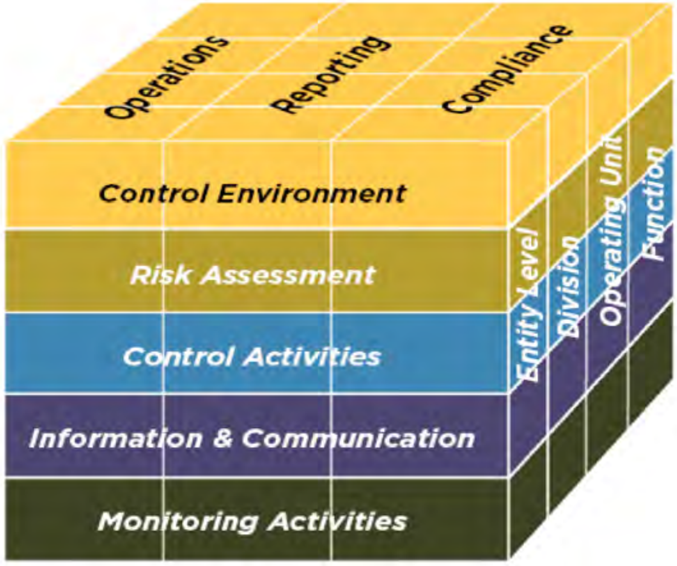
COSO FRAMEWORK RELATIONSHIP OF OBJECTIVES AND COMPONENTS

The COSO framework comprises three dimensions—objectives, components and organizational structure of an entity—in a cube model, as illustrated in **figure 2**.

"A direct relationship exists between objectives, which are what an entity strives to achieve, *components*, which represent what is required to achieve the objectives, and the *organizational structure* of the entity (the operating units, legal entities, and other). The relationship can be depicted in the form of a cube.

- The three categories of objectives—operations, reporting, and compliance—are represented by the columns.
- The five components are represented by the rows.
- An entity's organizational structure is to be represented by the third dimension."[6]

Figure 2—COSO Framework Objectives, Components and Organization Structure Model



Source: COSO, *Internal Control—Integrated Framework Executive Summary*, USA, May 2013. Used with permission.

[6] *Op cit* COSO, May 2013

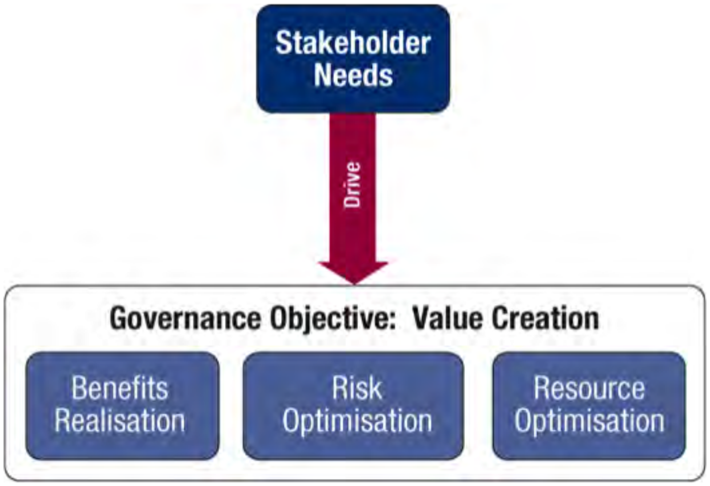
Reservation of Rights© 2014 ISACA. All rights reserved.

COBIT 5 Framework Relationship of Components and Content

The COSO Internal Control—Integrated Framework provides a sound basis from which to establish and assess internal control arrangements, using the model in **figure 2**, to integrate its dimensions. Likewise, the COBIT 5 framework provides a sound basis from which to establish, improve and assess GEIT arrangements, based on the following four key models, shown in **figures 3** through **6**.

- Value Creation—The overall COBIT governance objective

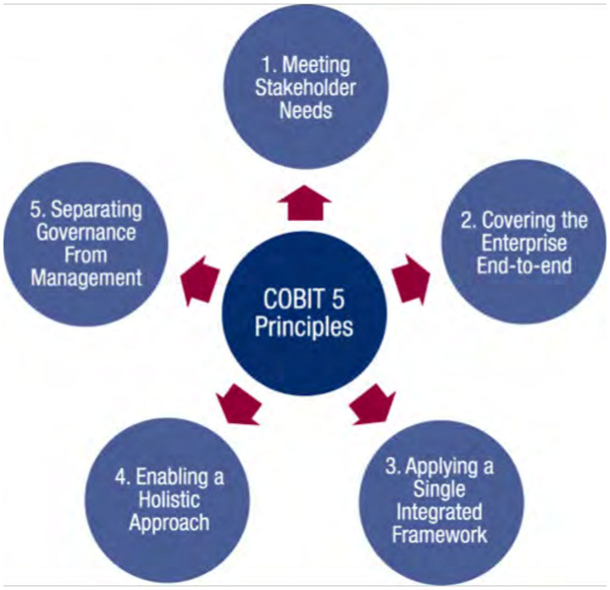
Figure 3—COBIT 5 Governance Objective: Value Creation Model



Source: ISACA, COBIT 5, USA, 2012, figure 3

- Five COBIT 5 principles

Figure 4—COBIT 5 Principles Model


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
COBIT 5 Principles

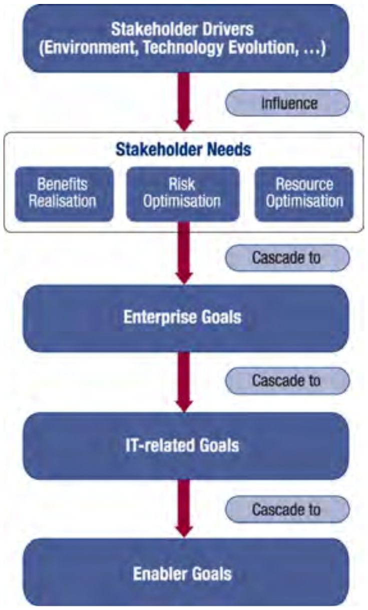
Source: ISACA, COBIT 5, USA, 2012, figure 2

Reservation of Rights© 2014 ISACA. All rights reserved.

COBIT 5 Framework Relationship of Components and Content (cont.)

- BSC-based goals cascade with business goals, IT-related goals and enabler goals

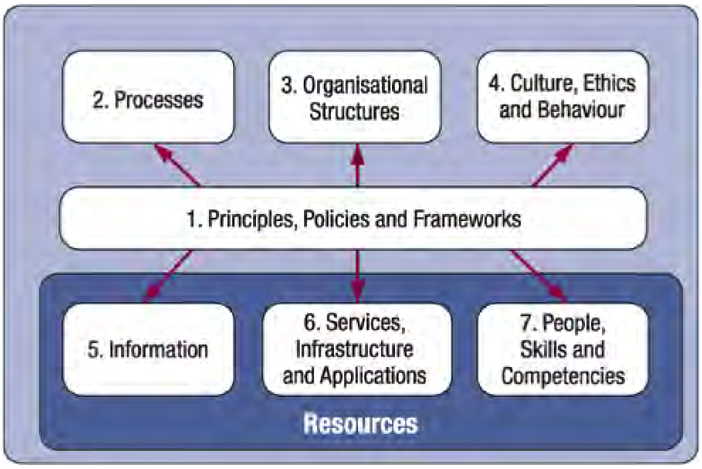
Figure 5—COBIT 5 Goals Cascade



Source: ISACA, *COBIT 5 for Assurance*, USA, 2013, figure 33

- Seven supporting enabler types

Figure 6—COBIT 5 Enterprise Enablers

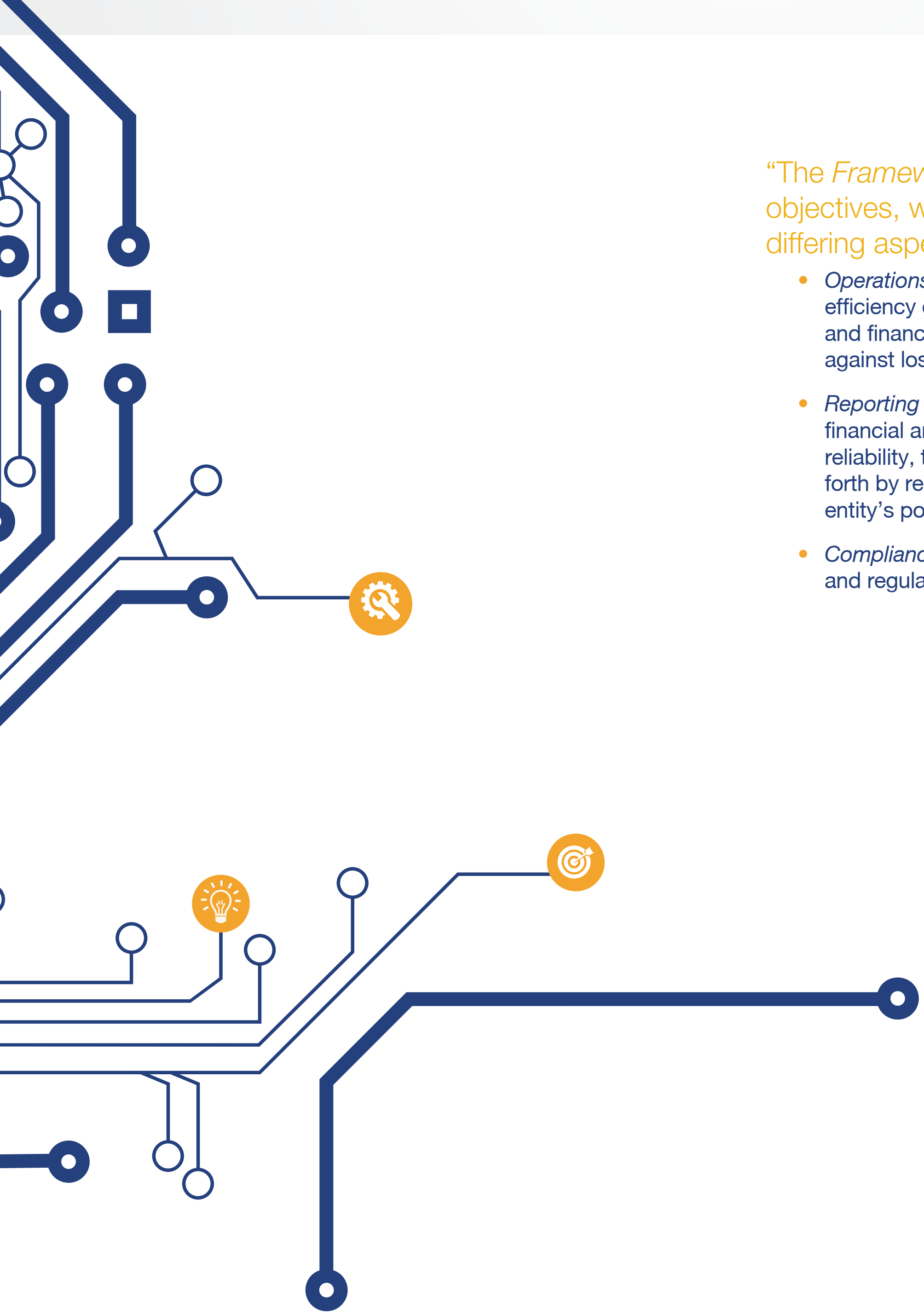

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Source: ISACA, COBIT 5, USA, 2012, figure 12

Note: The COBIT enabler models are described in the freely available COBIT 5 publication, which can be found at the COBIT web site *www.isaca.org/COBIT*.

Reservation of Rights© 2014 ISACA. All rights reserved.

COSO FRAMEWORK OBJECTIVES



"The *Framework* provides for three categories of objectives, which allow organizations to focus on differing aspects of internal control:

- *Operations Objectives*—These pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.
- *Reporting Objectives*—These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.
- *Compliance Objectives*—These pertain to adherence to laws and regulations to which the entity is subject."[7]

[7] *Op cit* COSO, May 2013

Reservation of Rights© 2014 ISACA. All rights reserved.

How COSO Framework Objectives Relate to COBIT 5 Framework Components and Content

COBIT 5 also focuses on enterprise objectives (referred to as goals), through the use of the goals cascade model. As shown in **figure 5**, the goals cascade includes enterprise, IT-related and enabler goals. The generic goals provided in the COBIT 5 guidance, for adaption by enterprises, are based on the four dimensions of the Kaplan and Norton Balanced Score Card (BSC)—Financial, Customer, Internal and Learning and Growth.[8] These dimensions, in turn, relate to the enterprise benefits realization, risk optimization and resource optimization objectives, which can be aligned with the COSO framework operations, reporting and compliance objectives.

The COBIT 5 framework relates to the COSO framework categories of objectives, as follows:

- **Operations**—COBIT is widely accepted as a best practice for governance and management of IT-related processes.
- **Reporting**—The COBIT 5 goals cascade and MEA domain processes support the COSO framework Reporting objective category.
- **Compliance**—The COBIT 5 process MEA03 external compliance-focused process and the COBIT 5 alignment with several relevant standards and frameworks[9] support the COSO framework Compliance objective category. COBIT is used as the basis for internal/external audits and regulatory guidance in certain locations and industries.

The 17 generic enterprise goals that are defined in COBIT 5 (**figure 7**) cover all aspects of operations goals across the four BSC dimensions. Enterprise reporting goals include financial transparency and information-based strategic decision making. Enterprise compliance goals include compliance with external laws and regulations and with internal policies.

Figure 7—COBIT 5 Enterprise Goals

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	**Risk Optimisation**	**Resource Optimisation**
Financial	1. Stakeholder values of business investment	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed bueinss chage programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Key: P = Primary, S = Secondary

Source: ISACA, COBIT 5, USA, 2012, figure 5

[8] *Op cit* Kaplan

[9] Relevant standards include the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series, and relevant frameworks include The Open Group Architecture Forum (TOGAF) 9 and Information Technology Infrastructure Library (ITIL) V3.

COSO FRAMEWORK PRINCIPLES AND COMPONENTS

"The *Framework* sets out seventeen principles representing the fundamental concepts associated with each component. Because these principles are drawn directly from the components, an entity can achieve effective internal control by applying all principles. All principles apply to operations, reporting, and compliance objectives."[10]

How COSO Framework Principles Relate to COBIT 5 Framework Components and Content

The COBIT 5 framework focuses on enterprise goals that create value for stakeholders through the use of the goals cascade model. This approach ensures that all stakeholder needs are identified and addressed by the governing body, which is the first COBIT 5 principle. The other four COBIT 5 principles (**figure 4**) support the COSO framework by setting the concepts for a sound framework for enterprise governance and management, and encompassing effective internal control to achieve enterprise goals.

Following are the five COSO components and their related principles, numbered 1 through 17. The related COBIT 5 framework components and content follow each COSO framework component description.

[10] *Op cit* COSO, May 2013

Reservation of Rights© 2014 ISACA. All rights reserved.

The COBIT 5 governance and management practices and other enabler guidance provide a sound and comprehensive basis for establishing an appropriate governance and management environment in the enterprise, i.e., an environment within which adequate processes and other enablers and supporting activities can be established and performed effectively. The COBIT 5 framework relationship to each of the numbered COSO framework Control Environment principles is shown in **figure 8**.

Figure 8—How COSO Framework Control Environment Principles Relate to COBIT 5 Framework Components and Content

COSO Principle[11]	COBIT 5 Relationship to COSO Principle
"1. The organization demonstrates a commitment to integrity and ethical values."	The COBIT 5 Culture, Ethics and Behaviour enabler addresses enterprise ethics and individual ethics and behaviors, including risk taking, by following policy and addressing negative outcomes. The COBIT 5 processes EDM01 *Ensure governance framework setting and maintenance* and APO01 *Manage the IT management framework* include activities to embed enterprise integrity and ethical value aspects within the governance and management framework. The COBIT 5 process APO07 *Manage human resources* includes activities to address integrity and ethical value aspects from a human resources perspective.
"2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control."	The COBIT 5 principle Separating Governance from Management supports the second COSO principle by differentiating governance and management disciplines and making independence easier to establish and maintain. In addition, all five COBIT 5 governance processes (EDM01 through EDM05) reinforce this separation in their RACI chart guidance.
"3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives."	The COBIT 5 Organisational Structure enabler addresses practices, such as operating principles, span of control (scope) definition, level of authority, delegation of authority powers and escalation paths, to support the establishment of effective organizational structures within enterprises. COBIT 5 process APO01 *Manage the IT management framework* includes activities to address the required definition of an organizational structure for the enterprise. APO01 takes direction from COBIT 5 process EDM01 *Ensure governance framework setting and maintenance* in respect to enterprise governance requirements.
"4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives."	The COBIT 5 People, Skills and Competencies enabler addresses the life cycle aspects that are related to people—knowing the current skills base; the skills that need to be retained, developed or acquired to meet enterprise goals; and the skills that can be disposed of when no longer needed. COBIT 5 process APO01 *Manage the IT management framework* includes activities to establish roles and responsibilities to support achievement of enterprise objectives. COBIT 5 process APO07 *Manage human resources* includes activities to address the attraction, development and retention of competent people.
"5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives."	The COBIT 5 Processes enabler and the RACI charts that support the 37 processes are particularly relevant in the context of individual accountability. The enabler and charts strongly advocate the assignment of responsibilities and accountabilities and provide examples of roles and responsibilities for the individual and group roles for all key GEIT-related processes and activities.

[11] *Ibid.*

Reservation of Rights© 2014 ISACA. All rights reserved.

The COBIT 5 framework and supporting guidance supports the enterprise objective of stakeholder value creation. One of the key areas of focus in delivering value is the optimization of business risk, applying appropriate risk treatment options to mitigate risk and keeping it within set appetite and tolerance levels. *The COBIT 5 for Risk*[12] professional guide provides specific guidance for risk assessment (and other risk-related aspects of IT governance and management) based on COBIT 5. The COBIT 5 framework relationship to each of the numbered COSO framework Risk Assessment principles is shown in **figure 9**.

Figure 9—How COSO Framework Risk Assessment Principles Relate to COBIT 5 Framework Components and Content

COSO Principle[13]	COBIT 5 Relationship to COSO Principle
"6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives."	The COBIT 5 framework focuses on enterprise objectives through the use of the goals cascade model, which is based on BSC theory. This model supports the enterprise by clearly defining its business objectives in a way that enables the identification and assessment of risk that relates to meeting objectives. The guidance for each of the 37 COBIT processes includes process goals (objectives).
"7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed."	The COBIT 5 Processes enabler guidance specifically addresses risk governance (process EDM03 *Ensure risk optimisation*) and management (process APO12 *Manage risk*). These processes include the practices and activities required to govern and manage risk effectively—including the identification, analysis and management of the risk. These processes drive other areas, e.g., information security and business continuity, which are addressed by other specific COBIT 5 processes.
"8. The organization considers the potential for fraud in assessing risks to the achievement of objectives."	The COBIT 5 framework does not focus on fraud as a specific business risk, although the guidance supports the establishment of a sound governance and management environment, within which practices and supporting activities can be established and performed to support effective fraud prevention activities. The specific inclusion of the COBIT 5 Culture, Ethics and Behaviour enabler helps to ensure that a culture that is fraud-risk-aware is established and that the consequences of engaging in such behavior are clearly communicated where appropriate. COBIT 5 processes EDM01, APO01 and APO07 support culture, ethics and behaviour objectives, including an enterprise's approach to fraud. COBIT process MEA03 *Monitor, evaluate and assess compliance with external requirements* should also be considered, because fraud prevention (bribery, privacy, etc.) is often part of an enterprise's external compliance requirements.
"9. The organization identifies and assesses changes that could significantly impact the system of internal control."	The COBIT 5 Processes enabler guidance specifically addresses changes in COBIT 5 process BAI06 *Manage changes*, which is directly linked to the IT-related goal "Managed IT-related business risk." This process, like the COSO principle, recognizes that changes within an enterprise can introduce risk and, therefore, need to be a focus from this perspective. Further, as changes occur in all areas of control activity (information, applications and general control activities over technology), these changes are addressed by various COBIT 5 processes. COBIT 5 process APO01 *Manage the IT management framework* addresses the management framework and manages changes to general controls. COBIT 5 process BAI06 *Manage changes* and, for programs and projects, COBIT 5 process BAI02 *Manage requirements definition* manage the changes to business processes, applications and infrastructure. All changes need to be tested and approved by following the COBIT 5 process BAI07 *Manage change acceptance and transitioning.* Impacts to business processes are handled according to COBIT 5 process BAI05 *Manage organisational change enablement.*

[12] ISACA, *COBIT 5 for Risk,* USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

[13] *Ibid.*

Reservation of Rights© 2014 ISACA. All rights reserved.

The COBIT 5 Processes enabler uses process practices and process activities to define good practice for IT. Process practices describe what a process needs to realize its goals in support of stakeholder (enterprise) goals and needs.

The COBIT 5 process model addresses a complete set of 37 required processes and the control activities that are relevant for sound internal control over information and related technology and are fully integrated with major IT-relevant global standards and good practices.[14]

Further, goals apply not only to Processes, but also to the other six enabler types in COBIT 5. Defined enabler goals support the effective implementation of governance and management practices, which support the achievement of those enabler goals and, ultimately, the achievement of the enterprise business goals.

The COBIT 5 framework relationship to each of the numbered COSO framework Control Activities principles is shown in **figure 10**.

Figure 10—How COSO Framework Control Activities Principles Relate to COBIT 5 Framework Components and Content

COSO Principle[15]	COBIT 5 Relationship to COSO Principle
"10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels."	The COBIT 5 Processes enabler guidance for the 37 COBIT 5 processes supports enterprises in their selection and development of control activities and other arrangements (e.g., structural segregation of duties), particularly with the practices and activities to consider for IT-related enterprise processes. This guidance includes how the IT-related enterprise process practices and activities support the IT-related goals of "Managed IT-related business risk," "IT compliance and support for business compliance with external laws and regulations" and "IT compliance with internal policies."
"11. The organization selects and develops general control activities over technology to support the achievement of objectives."	The COBIT 5 principles and enablers can be applied to the governance and management of any type of enterprise activity as described in the previous paragraph (COSO principle 10). Detailed COBIT 5 guidance relates generically to the governance and management of information and information technology assets. As such, the detailed guidance in COBIT 5 is directly supportive of COSO principle 11, "selects and develops general control activities over technology."[16] Control activities can be process activities within all of the 37 COBIT processes or relate to other enabler types. In particular, COBIT 5 process DSS06 *Manage business process controls* ensures that control activities that are embedded in business processes (automated controls or application controls) are adequately managed.
"12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action."	The COBIT 5 Principles, Policies and Frameworks enabler is central to effective enterprise IT governance and management. Enterprise policies are central to COBIT 5 support of achievement of enterprise goals, including mitigation of risk through the use of appropriate activities. COBIT 5 process APO01 *Manage the IT management framework* includes activities that address the implementation of enterprise policies.

[14] The global standards and good practices that are relevant to IT include TOGAF, ISO/IEC 27000, ITIL, PRojects IN Controlled Environments (PRINCE2) and Project Management Body of Knowledge (PMBOK).

[15] *Op cit* COSO, May 2013

[16] *Ibid.*

Reservation of Rights© 2014 ISACA. All rights reserved.

In COBIT 5, Information is a part of the overall focus of the governance and management framework (information and related technology are enterprise assets) and a supporting enabler with associated attributes.

Facilitating effective communication, by providing a common-language framework for GEIT, is a key purpose of COBIT 5.

The COBIT 5 framework relationship to each of the numbered COSO framework Information and Communication principles is shown in **figure 11**.

Figure 11—How COSO Framework Information and Communication Principles Relate to COBIT 5 Framework Components and Content

COSO Principle[17]	COBIT 5 Relationship to COSO Principle
"13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control."	The COBIT 5 Information enabler model describes 15 Information quality goals, which are categorized into intrinsic, contextual and security/accessibility quality dimensions. Considering each quality goal helps enterprises to ensure that the information used supports enterprise business goals, including control objectives. The guidance for the 37 COBIT 5 processes includes inputs and outputs that are the communication of information across, and to and from, the enterprise. In particular, COBIT 5 process MEA01 *Monitor, evaluate and assess performance and conformance* addresses performance and conformance data, and COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control* addresses control effectiveness reviews.
"14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control."	The COBIT 5 framework provides sound, structured and comprehensive guidance that facilitates effective internal communication of GEIT aspects and issues between the multiple internal stakeholders. This includes the communication of clear objectives that result from the goals cascade, including Processes enabler goals (objectives), which are provided for all 37 COBIT 5 processes. The need to communicate information with stakeholders as part of enterprise process design and execution, to support the achievement of process and related business goals, is addressed in the RACI charts, with the responsibilities of "consult" and "inform," and the input and output suggestions that support the process guidance for the 37 COBIT 5 processes. This communication is implemented and managed following COBIT 5 process APO01 *Manage the IT management framework.* In addition, a comprehensive guide, *COBIT 5 Implementation,* is available.
"15. The organization communicates with external parties regarding matters affecting the functioning of internal control."	The COBIT 5 framework also provides a sound basis for effective communication of GEIT aspects and issues to external stakeholders when appropriate. In particular, the COBIT 5 process EDM05 *Ensure stakeholder transparency* requires that the communication to stakeholders is effective and timely and that a reliable, consistent basis for reporting is established.

[17] *Ibid.*

Reservation of Rights© 2014 ISACA. All rights reserved.

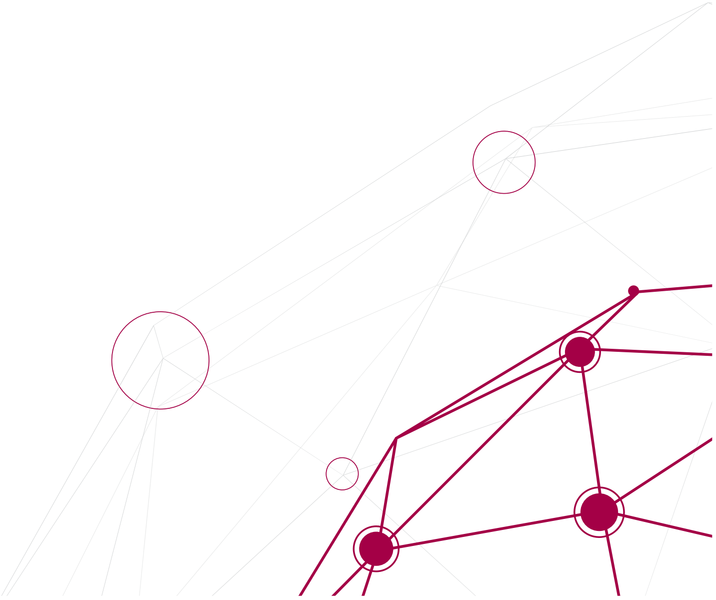
In COBIT 5, monitoring to ensure that enterprise business goals are met is a main focus of the framework.

The Processes enabler domain Monitor, Evaluate and Assess (MEA) is dedicated to this type of management activity. This domain contains three processes that monitor, evaluate and assess performance and conformance; the system of internal control; and compliance with external requirements. Monitoring is also a key activity within each of the five governance (Evaluate, Direct and Monitor [EDM]) processes.

The COBIT 5 framework relationship to each of the numbered COSO framework Monitoring Activities principles is shown in **figure 12.**

Figure 12—How COSO Framework Monitoring Activities Principles Relate to COBIT 5 Framework Components and Content

COSO Principle[18]	COBIT 5 Relationship to COSO Principle
"16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning."	The COBIT 5 Processes enabler guidance specifically addresses monitoring, evaluation and assessment of internal control adequacy (COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control)*. This process includes the practices and activities that are required to monitor internal controls; review business process controls effectiveness; perform control self-assessments; identify and report control deficiencies; ensure that assurance providers are independent and qualified; and plan, scope and execute assurance activities.
"17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate."	As noted in the previous paragraph, COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control* includes the practices and activities that are required to identify control deficiencies; analyze and identify their underlying root cause; escalate control deficiencies; and report to stakeholders as appropriate. In addition, COBIT 5 process EDM05 *Ensure stakeholder transparency* includes practices and activities to evaluate, direct and monitor stakeholder reporting and communication requirements, including those that are related to control deficiencies, to senior management and the board, as appropriate.



[18] *Ibid.*

Reservation of Rights© 2014 ISACA. All rights reserved.

CONCLUSION

Many enterprises ask, “With the update of both the COSO Internal Control–Integrated Framework and the COBIT framework, are they still complementary and compatible?” The answer to this question is yes, **the frameworks are complementary and compatible as guidance to support the assessment and improvement of internal control practices and activities within the governance and management arrangements of an enterprise.** Goals of both the COSO and the COBIT framework updates and refreshes are to further clarify the enterprise principles on which effective internal control environment and activities should be based and to provide a focus on the enterprise governance and management enablers that need to be addressed to deliver the required business objectives/goals to the stakeholders. Use of both frameworks continues to require professional judgment and work by enterprise management and its auditors/advisors to comprehend, adapt and apply the principles and guidance to specific enterprise goals and enterprise capabilities.

This white paper provides a high-level explanation of how the two widely used frameworks align and the value of using COSO and COBIT together. **The COSO framework provides very useful principles on internal control; the COBIT 5 framework provides additional guidance on the information- and technology-related governance and management enablers that are critical to the operation of internal financial controls in enterprises.** ISACA anticipates additional thinking regarding the benefits and usefulness of both frameworks and looks forward to observing further discussions about how enterprises are using these two globally accepted frameworks together.

Note: Additional information about COSO and how to obtain the framework can be found at the COSO web site, *www.coso.org/ic.htm*. Likewise, the COBIT framework and supporting guidance, training materials and sources can be found at the COBIT web site *www.isaca.org/COBIT*.

APPENDIX—RELATIONSHIP BETWEEN THE COSO PRINCIPLES AND COBIT 5 PROCESS GUIDANCE

COSO Principle and Description[19]		COBIT Process Reference	Relationship to COSO Principle
Control Environment			
1	The organization demonstrates a commitment to integrity and ethical values.	EDM01 APO01 APO07	COBIT 5 processes EDM01 *Ensure governance framework setting and maintenance* and APO01 *Manage the IT management framework* include activities to embed enterprise integrity and ethical value aspects within the governance and management framework. COBIT 5 process APO07 *Manage human resources* includes activities to address integrity and ethical value aspects from a human resources perspective.
2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	EDM01-05	All five COBIT governance processes (EDM01 through EDM05) reinforce this separation in their RACI chart guidance.
3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	EDM01 APO01	COBIT 5 process APO01 *Manage the IT management framework* includes activities to address the required definition of an organizational structure for the enterprise. APO01 takes direction from process EDM01 *Ensure governance framework setting and maintenance* regarding enterprise governance requirements.
4	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	APO01 APO07	COBIT 5 process APO01 *Manage the IT management framework* includes activities to establish roles and responsibilities to support achievement of enterprise objectives. COBIT 5 process APO07 *Manage human resources* includes activities to address the attraction, development and retention of competent people.
5	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	All COBIT 5 Processes	The COBIT 5 Processes enabler and supporting RACI charts for all 37 processes are particularly relevant to the context of individual accountability. The enabler and charts strongly advocate the assignment of responsibilities and accountabilities and provide examples roles and responsibilities for key individual and group roles for all key GEIT-related processes and activities.
Risk Assessment			
6	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	All COBIT 5 Processes	The guidance for all 37 COBIT 5 processes includes process goals (objectives).
7	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	EDM03 APO12	The COBIT 5 Processes enabler guidance specifically addresses risk governance (process EDM03 *Ensure risk optimisation*) and management (process APO12 *Manage risk)*. These processes include the practices and activities that are required to govern and manage risk effectively, including their identification, analysis and management.

[19] COSO, "Internal Control—Integrated Framework Executive Summary", May 2013, *www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf.* Used with permission.

Reservation of Rights© 2014 ISACA. All rights reserved.

COSO Principle and Description[19]		COBIT Process Reference	Relationship to COSO Principle
Risk Assessment			
8	The organization considers the potential for fraud in assessing risks to the achievement of objectives.	EDM01 APO01 APO07 MEA03	COBIT 5 processes EDM01, APO01 and APO07 support culture, ethics and behavior objectives, including an enterprise's approach to fraud. COBIT 5 process MEA03 *Monitor, evaluate and assess compliance with external requirements* should also be considered, because fraud prevention (bribery, privacy, etc.) is often part of an enterprise's external compliance requirements.
9	The organization identifies and assesses changes that could significantly impact the system of internal control.	APO01 BAI02 BAI05 BAI06 BAI07	The COBIT 5 Processes enabler guidance specifically addresses changes in the COBIT 5 process BAI06 *Manage changes*, which is directly linked to the IT-related goal "Managed IT-related business risk." This process, like the COSO principle, recognizes that changes within an enterprise can introduce risk and, therefore, need to be a focus from this perspective. Further, as changes occur in all areas of control activity (information, applications and to general control activities over technology), these changes are addressed by different COBIT 5 processes. COBIT 5 process APO01 *Manage the IT management framework* addresses the management framework and manages changes to general controls. COBIT 5 process BAI06 *Manage changes* and, for programs and projects, COBIT 5 process BAI02 *Manage requirements definition* manage the changes to business processes, applications and infrastructure. All changes need to be tested and approved by following the *COBIT 5 process* BAI07 *Manage change acceptance and transitioning*. Impacts to business processes are handled according to COBIT 5 process BAI05 *Manage organisational change enablement.*
Control Activities			
10	The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	All COBIT 5 Processes	The COBIT 5 Processes enabler guidance for the 37 COBIT 5 processes supports enterprises in their selection and development of control activities and other arrangements (e.g., structural segregation of duties), particularly with the practices and activities to consider for IT-related enterprise processes.
11	The organization selects and develops general control activities over technology to support the achievement of objectives.	All COBIT 5 Processes	Control activities can be process activities within all of the 37 COBIT 5 processes. In particular, COBIT 5 process DSS06 *Manage business process controls* ensures that control activities embedded in business processes (automated controls or application controls) are adequately managed.
12	The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	APO01	COBIT 5 process APO01 *Manage the IT management framework* includes activities that address the implementation of enterprise policies.
Information and Communication			
13	The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.	All COBIT 5 Processes	The guidance for the 37 COBIT 5 processes includes inputs and outputs that are the communication of information across, and to and from, the enterprise. In particular, COBIT 5 process MEA01 *Monitor, evaluate and assess performance and conformance* addresses performance and conformance data, and COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control* addresses control effectiveness reviews.

[19] COSO, "Internal Control—Integrated Framework Executive Summary", May 2013, *www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf.* Used with permission.

Reservation of Rights© 2014 ISACA. All rights reserved.

COSO Principle and Description[19]		COBIT Process Reference	Relationship to COSO Principle
Information and Communication			
14	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	All COBIT 5 Processes	Processes enabler goals (objectives) are provided for all 37 COBIT 5 processes. The need to communicate information with stakeholders as part of enterprise process design and execution, to support the achievement of process and related business goals, is addressed in the RACI charts, with the responsibilities of “consult” and “inform,” and the input and output suggestions that support the process guidance for the 37 COBIT 5 processes. This communication is implemented and managed following COBIT 5 process APO01 *Manage the IT management framework.*
15	The organization communicates with external parties regarding matters affecting the functioning of internal control.	EDM05	COBIT 5 process EDM05 *Ensure stakeholder transparency* ensures that the communication to stakeholders is effective and timely and that a reliable, consistent basis for reporting is established.
Monitoring Activities			
16	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	MEA02	The COBIT 5 Processes enabler guidance specifically addresses monitoring, evaluation and assessment of internal control adequacy (COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control*). This process includes the practices and activities that are required to monitor internal controls; review business process controls effectiveness; perform control self-assessments; identify and report control deficiencies; ensure that assurance providers are independent and qualified; and plan, scope and execute assurance activities.
17	The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	EDM05 MEA02	COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control* includes the practices and activities that are required to identify control deficiencies; analyze and identify their underlying root cause; escalate control deficiencies; and report to stakeholders as appropriate. In addition, COBIT 5 process EDM05 *Ensure stakeholder transparency* includes practices and activities to evaluate, direct and monitor stakeholder reporting and communication requirements, including those related to control deficiencies, to senior management and the board, as appropriate.

[19] COSO, “Internal Control—Integrated Framework Executive Summary”, May 2013, *www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf.* Used with permission.