FEATURE

Technology's Role in Enterprise Risk Management

亦有中文简体译本
www.isaca.org/currentissue

The new COSO ERM framework document, *Enterprise Risk Management—Integrating With Strategy and Performance*,[1] is expected to have a level of global influence similar to *Internal Control–Integrated Framework*.[2] The ERM framework is designed to provide reasonable expectation that an entity that adopts it understands and manages all kinds of risk associated with business strategy and performance objectives. It provides a strong foundation for integrating the management of all types of risk. Technology innovation is acknowledged as a key enabler for strategy decision support and an example of a strategic business objective. Technology risk is one of many examples of enterprise risk the document uses to illustrate the ERM framework.

Framework Synergies

Like COBIT 5, the COSO ERM framework is principles-based and emphasizes that strategic plans to support the mission and vision of an organization must be supported with governance elements, performance measurement and internal control. It describes how risk managers in all professions weigh the probability that activities prompted by a given strategy may result in foreseeable future events that impact an entity's mission. Also like COBIT 5, the COSO ERM framework advocates continuous process improvement that relies heavily on governance structures to assist in framing decisions.

ERM framework principles operate as closed-loop systems. Although the specific list of principles differs, both frameworks speak to objective setting, risk prioritization, information system leverage, monitoring and reporting. Just as depicted by the COBIT 5 goals cascade (**figure 1**), some ERM components must be established in cascading order to provide goals for others, but, once established, there is no prescribed sequential order for the continuous operation of risk management activities. Just as depicted by the information flow of COBIT 5 (**figure 2**), processes occur simultaneously and rely on shared information to form a holistic approach to risk management. At a more granular level, the principles are also familiar to cybersecurity professionals who are familiar with prevent-detect-recover, observe-orient-decide-act and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework's identify-protect-detect-respond-recover loops. These all have components that rely on shared goals and strategies and are expected to run simultaneously and support each other.

The corresponding COSO ERM framework diagram appears in **figure 3**. As in the COBIT 5 goals cascade, strategy follows from stakeholder values, and business-related objectives and performance goals follow from enterprise goals. As in the COBIT 5 information flow, information flows from

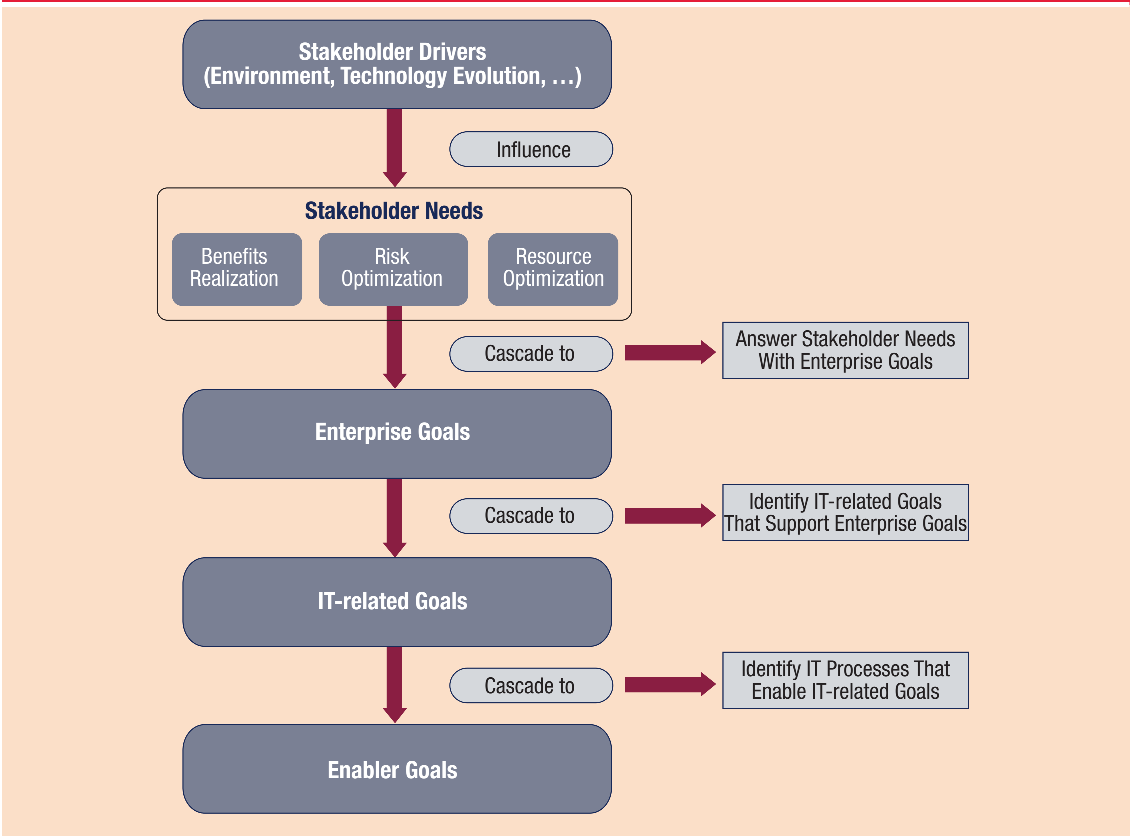
Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2rY4UVJ

Jennifer Bayuk, CISA, CISM, CGEIT
Is a frequent ISACA author and volunteer. She represented ISACA on the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management Framework Committee.

Figure 1—COBIT 5 Goals Cascade


Stakeholder Drivers
(Environment, Technology Evolution, …)
Influence
Stakeholder Needs
Benefits Realization
Risk Optimization
Resource Optimization
Cascade to
Answer Stakeholder Needs With Enterprise Goals
Enterprise Goals
Cascade to
Identify IT-related Goals That Support Enterprise Goals
IT-related Goals
Cascade to
Identify IT Processes That Enable IT-related Goals
Enabler Goals

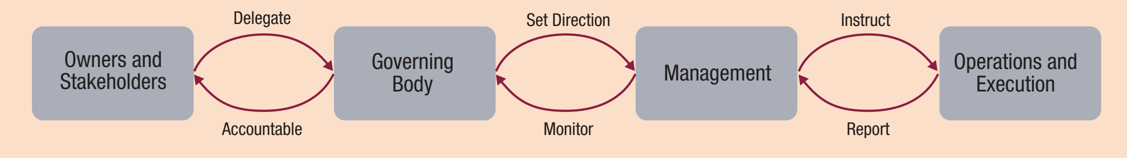
Source: ISACA, COBIT 5, USA, 2012. Reprinted with permission.

stakeholders to governors to management to enablers and back. It is important for technology professionals to understand that ERM framework components are not just paper exercises, but are enterprise-level frameworks that can be leveraged to frame decisions in support of technology risk management objectives. Particularly in the dimensions of governance, strategy and reporting, if technology risk is managed independently of ERM, it is not as likely to be supported from the top down with professional risk management resources.

The key to effective design and implementation of a technology risk management framework is to recognize that ERM framework components are understood at the board level and to leverage the strengths of the board-level ERM program within the organization to support technology risk management. Of course, there has always been guidance that technology professionals should engage senior management in addressing technology risk. The difference in this version of COSO's guidance is that it is becoming far more obvious that ERM professionals have a professional obligation to meet technology professionals more than halfway. Although in the past it may have seemed to technology risk professionals that higher-level ERM activities within their organization take technology risk management for granted, this scenario has changed and is rapidly evolving. Cybersecurity threats and other disruptive technology concerns are top of mind for today's board members.[3]

> “THE COSO ERM FRAMEWORK ADVOCATES CONTINUOUS PROCESS IMPROVEMENT THAT RELIES HEAVILY ON GOVERNANCE STRUCTURES TO ASSIST IN FRAMING DECISIONS.”

Figure 2—COBIT 5 Information Flow



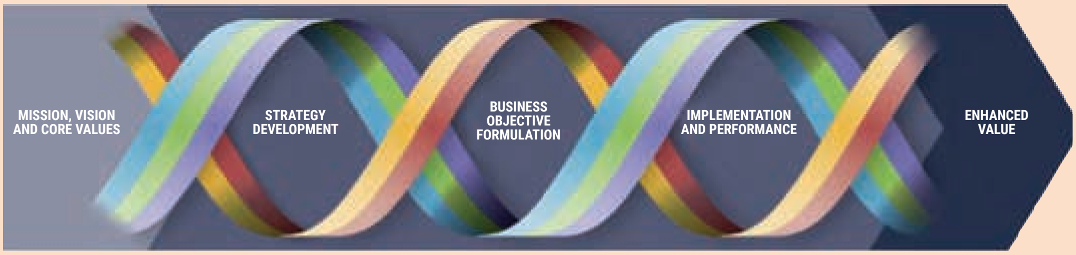
Source: ISACA, *COBIT® 5: Enabling Information*, USA, 2013. Reprinted with permission.

In all large enterprises, and in many midsized ones, ERM has long been a formal endeavor to ensure that the mission, vision and core principles of the firm are the basis of strategic planning. These activities drive resource allocation and decision support, clearly articulating the tone at the top. Technology strategy planning, however, often originates with goals of lower-level objectives such as infrastructure migrations, people location strategies, cost cutting and/or development timeline reduction. These are not strategic goals that cascade directly from enterprise mission and values, and sometimes conflict with the technology activities that would more directly support those values. For example, a cost-cutting initiative wherein development activities are targeted to be outsourced may conflict with a goal to streamline customer experience, as the latter goal would require close collaboration among development teams in different business areas. In recognition that the activities of enterprise risk have not always been particularly transparent to stakeholder organizations such as technology, the COSO ERM framework begins with a thorough explanation of the underlying dynamics that are expected to occur between the board and executive management in defining an approach to ERM. It starts with a definition of enterprise risk management: "the culture, capabilities and practices, integrated with strategy setting and performance, that organizations rely on to manage risk in creating, preserving and realizing value."[4]

As the definition spans multiple complex concepts, each concept is described in the context of the challenges inherent in managing risk at the enterprise level. Many of these challenges are also described in COBIT 5. **Figure 4** specifies the sections in both documents that show how the COSO ERM definition relates to COBIT's key principles for governance and management of enterprise IT.[5, 6]

Figure 3—COSO Enterprise Risk Management, Components and Principles

ENTERPRISE RISK MANAGEMENT


MISSION, VISION AND CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION AND PERFORMANCE
ENHANCED VALUE

Governance and Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Developes, and Retains Capable Individuals

Strategy and Objective Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risk
13. Implements Risk Responses
14. Develops Portfolio View

Review and Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, and Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO, *Enterprise Risk Management: Integrating With Strategy and Performance*, USA, 2017. Reprinted with permission.

Figure 4—How COSO's ERM Definition Relates to COBIT Key Principles for Governance and Management of Enterprise IT

COSO ERM	COBIT 5
Recognizing culture, developing capabilities	Establishing a holistic approach (Principle 4)
Applying practices	Applying a single, integrated framework (Principle 3)
Integrating with strategy setting and performance	Covering the enterprise end-to-end (Principle 2)
Managing risk to strategy and business objectives	Separating governance from management (Principle 5)
Linking to value	Meeting stakeholder needs (Principle 1)

Although both frameworks are principle-based, and appear similar at a high level, COSO ERM is a higher-level framework as it encompasses consideration of all types of risk, including technology risk. Nevertheless, like COBIT 5, it emphasizes the importance of management unity at the framework level and emphasizes that alignment and integration of potentially separate frameworks are the shortest path to improved decision support.[7, 8]

As depicted in **figure 3**, the COSO ERM framework includes 20 principles that are grouped into five framework components:

1. Governance and culture
2. Strategy and objective setting
3. Performance
4. Review and revision
5. Information, communication and reporting

COBIT 5's principles do not map to COSO ERM's principles, but to the technology environment in which ERM's principles operate. That is, the ERM component principles are observed in the definition and execution of COBIT 5's deep dives into the special issues inherent in technology risk management at the COBIT 5 enabler level, rather than at the COBIT 5 framework level.

This is particularly true for the COBIT 5 process enabler, which contains COBIT 5's most prescriptive guidance specific to risk management.[9] COBIT 5 thus delivers more detailed guidance for technology professionals for the successful application of both the COBIT 5 framework and the ERM framework principles. **Figure 5** specifies the sections in both documents that show how COSO framework components and principles relate to COBIT 5 enablers.

“COBIT 5'S PRINCIPLES DO NOT MAP TO COSO ERM'S PRINCIPLES, BUT TO THE TECHNOLOGY ENVIRONMENT IN WHICH ERM'S PRINCIPLES OPERATE.”

Risk Information Enabler

The last four rows of **figure 5** specify the sections in both documents that show how COSO ERM performance principles relate to COBIT 5 process enabler APO12 Manage Risk—Key Practices. It shows that, in both COSO ERM and COBIT 5, there is an expectation that risk management relies on data collection and use of that data in risk analysis, risk articulation and risk profiling. This highlights the critical dependency or ERM on risk management information collected in the course of running business processes. It thus puts a spotlight on risk information systems that are increasingly reliant on business analytics tools to provide reports and calculate potential losses based on risk models.

As business analytics systems have become more popular and widespread, data gathering has often been placed in the hands of risk analysts, with the result that end-user computing has become a

Figure 5—How COSO Framework Components Relate to COBIT Enablers

COSO ERM Component/Principle	COBIT 5 Primary Corresponding Enabler
Component 1. Governance and Culture	Culture, Ethics and Behavior Enabler
Component 2. Strategy and Objective Setting	Process Enabler: EDM03.01 Evaluate Risk Management Process Enabler: EDM03.02 Direct Risk Management Process Enabler: APO02 Manage Strategy
Component 3. Performance	Process Enabler: APO12 Manage Risk Process Enabler: MEA01.01 Monitor, Evaluate and Assess Performance and Conformance
Component 4. Review and Revision	Information Enabler: Contextual and Representational Goals for Risk Profile Information Item
Component 5. Information, Communication and Reporting	Information Enabler: Information Model Process Enabler: EDM03.03 Monitor Risk Management Process Enabler: MEA01.02 Monitor, Evaluate and Assess the System of Internal Control.
Principle 10. Identifies Risk	Process Enabler: APO12.01 Collect Data (key output—risk issues and factors)
Principle 11. Assesses Severity of Risk	Process Enabler: APO12.02 Analyze Risk
Principle 12. Prioritizes Risk	Process Enabler: APO12.04 Articulate Risk
Principle 13. Implements Risk Responses	Process Enabler: APO12.05 Define a Risk Management Action Portfolio Process Enabler: APO12.06 Respond to Risk
Principle 14. Develops Portfolio View	Process Enabler: APO12.03 Maintain a Risk Profile
Principle 18. Leverages Information Systems	Information Enabler: Enabling Information for Risk Management
Principle 19. Communicates Risk Information	Process Enabler: EDM01.02 Direct the Governance System Process Enabler: APO08 Manage Relationships
Principle 20. Reports on Risk, Culture and Performance	Process Enabler: EDM03.03 Monitor Risk Management

de facto mode of operation in many risk management departments. Even when their business analytic engines are server-based or use big data analytic software, the risk information databases are often populated with spreadsheets downloaded by risk analysts from a wide variety of disparate systems. Risk analysts sometimes download data without indexes and deal with record-mapping problems by creating their own translation table and formulas. Where multiple such systems exist in the same organization, it is hard to aggregate data across multiple risk domains, and aggregation tools sometimes depend on mapping as well. This situation is so widespread that the Bank of International Settlements produced specific guidance on risk aggregation reporting.[10] This critical dependency on information technology is called out in the COSO ERM framework. That is, the risk that technology supporting ERM may itself be flawed is brought to the highest level of enterprise risk awareness, setting forth a condition for the integration of ERM capabilities as: "When making necessary investments in technology or other infrastructure, management considers the tools required **to enable** enterprise risk management activities"[11] (emphasis added).

The strategic importance of maintaining business analytics systems correctly and effectively is finally getting the board-level attention it deserves. Data structures used to represent the enterprise, its business units and organizational structures are fundamental components of risk management information architecture, and consistency of such structures across risk management domains is essential to complete an accurate profile at the enterprise level.

COBIT 5 addresses this problem in a general manner that is relevant to any business process in the *COBIT® 5: Enabling Information* publication.[12] It describes information as composed of physical, empirical, semantic, pragmatic dimensions that should be transparently articulated. It distinguishes information life cycles into phases for plan, design, build/acquire, use/operate, monitor and dispose. It emphasizes the importance of offsetting quality requirements and corresponding goals. It is the special role of the technology risk management professional to use such tools and techniques to protect the integrity of that information design and data-gathering process for all risk information, not just that related to technology risk. Happily for a technology risk management audience, *COBIT 5: Enabling Information* uses a risk profile as an example of an information item, and provides illustrative data content, information life cycle roles and responsibilities, and quality goals for the risk profile information item.[13]

Key Takeaways

Where technology risk management is aligned with corporate risk management organizations conducting ERM activities at the board level, technology strategic plans may be expected to be in lockstep with the enterprise's mission, vision and core principles. The COSO ERM and COBIT 5 frameworks represent a body of knowledge shared across a large community of practitioners that may be utilized to create that alignment. Technology and cybersecurity risk and audit professionals should be conversant with both frameworks, and be familiar with the integration touchpoints between them. Key takeaways from this overview include:

- Effective technology risk management requires that the ERM framework encompass technology.
- As technology risk management professionals are specialists in risk related to information integrity and availability, they play a special role in ERM. The processes they use to identify, assess, quantify and monitor technology risk apply not just to risk in the technology or cybersecurity category, but should be designed to support the integrity of information used by risk managers in other risk domains.
- Technology professionals are uniquely positioned to identify issues related to risk aggregation strategies, and to support ERM activities with information life cycle process and quality control objectives.
- Where both COSO ERM and COBIT 5 are explicitly used by an organization, both enterprise risk and technology professionals should be educated on how they are compatible and why they should be used together and not separately.

Enjoying this article?

- Read *Getting Started With Risk*. *www.isaca.org/getting-rtarted-with-risk*
- Learn more about, discuss and collaborate on information security management in the Knowledge Center. *www.isaca.org/information-secuirty-management*

Endnotes

[1] In 2014, ISACA and other similarly influential associations affiliated with other risk-management-related professions were invited to participate in a committee focused on enhancing enterprise risk management (ERM) guidance provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which was first published in 2004. COSO is an independent private-sector association sponsored jointly by five major professional associations focused on financial statement integrity: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA). COSO's goal is to provide thoughtful leadership dealing with three interrelated subjects: ERM, internal control and fraud deterrence.

[2] COSO's flagship publication, *Internal Control–Integrated Framework*, is also a product of widespread collaboration across numerous industry associations and private sector contributors, and is the foundation for most global organizations' internal control frameworks. There was a multiyear effort when it was first published in 1992, and in a subsequent update in 2013. ISACA participated in that update committee as well.

[3] National Association of Corporate Directors, Resource Center: Emerging Issues, USA, 2018 *https://www.nacdonline.org/Resources/BoardResource.cfm?ItemNumber=38149*

[4] The Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management: Integrating With Strategy and Performance*, USA, 2017, *https://www.coso.org/Pages/ERM-Framework-Purchase.aspx*

[5] *Ibid*.

[6] ISACA, *Relating the COSO Internal Control—Integrated Framework and COBIT®*, USA, 2013, https://*www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Relating-the-COSO-Internal-Control-Integrated-Framework-and-COBIT.aspx*

[7] *Op cit* COSO 2017

[8] *Op cit* ISACA 2013

[9] ISACA, *COBIT 5: Enabling Processes*, USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*

[10] Basel Committee on Banking Supervision, *Principles for Effective Risk Data Aggregation and Risk Reporting*, Bank for International Settlements, January 2013, *www.bis.org/publ/bcbs239.pdf*

[11] *Op cit* COSO, 2017, p. 19

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

[13] *Ibid*.